An Adaptive Trustworthiness Modelling Approach for Ubiquitous Software Systems

Amr Ali-Eldin, Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt

Jan Van Den Berg, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, Netherlands

Semir Daskapan, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, Netherlands

ABSTRACT

With the growing interest in ubiquitous applications, attention should be given to privacy and trust issues. Since these environments are quite dynamic, and interactive where devices possess low computing resources, new trust models are required that suit this environment and help overcome its limitations. In this paper, the authors explore the possibility to settle trust in an adaptive way prior to any information disclosure to enable adaptive privacy and security. The proposed model is simulated in a commercial cluster scenario where users can clear all their payments with their short-range ubiquitous devices. In this domain, the authors assume that the user has to rely on what they call payment disclosure service (PDS) to control his or her disclosure decisions. The proposed model respects the limitations of wireless devices such as limited connectivity and processing resources, while enabling autonomous and secure operations.

Keywords: Context-Awareness, Privacy, Security Payment Models, Trustworthiness, Ubiquitous Software Systems

INTRODUCTION

Recently, it has been noticed that wireless and mobile technology networks have evolved enormously paving the way for a new paradigm known as ubiquitous computing. Examples of ubiquitous applications include the Internet of Things (IOTs), smart cities, location-based mobile applications and context-aware systems. A ubiquitous network can be seen as a telecommunications network that connects a collection of things, objects or devices to allow communication and data exchange between systems, software applications, and users. Besides, ubiquitous environments include software agents, services, and applications, which are expected to seamlessly interact and exchange user sensitive information with each other. In addition, devices are

DOI: 10.4018/IJISP.2014100103
embedded in physical objects and can collect sensitive information without human intervention (Denko, Sun et al. 2011).

The use of wireless technology is increasing rapidly, not only in the more developed countries, but also in developing countries, which have poor telecommunications infrastructures. Accordingly, a wide range of short range mobile services is being developed and the prospective developments are even more promising. Whereas in the past a customer had to be physically present at a certain time and at a certain place to meet with his or her friends, now he or she can do much of the social part from behind his or her computer or smart phone through the use of social mobile applications. Integration of several wireless technologies, i.e., short range or proximity area networks (PANs), wireless local area networks (WLANs) and 4G/5G mobile telecommunication networks and wireless wide area networks (WWN), lead to meshed wireless networks (MWNs), which enable even better ways to meet users’ needs anywhere and everywhere (Malladi and Agrawal 2002, Choi, Crowgey et al. 2006).

Ubiquitous applications represent another opportunity for the mobile industry and the financial institutions, since they bring convenience, flexibility and simplicity for the consumers (Daskapan, Berg et al. 2010). Despite the expected benefits behind these new developments, privacy and trust issues represent important challenges for the success and widespread adoption of these services (Ali-Eldin 2011, DasGupta and Chaki 2015). Trustworthiness of the service providers that collect information and offer their services represent a specific concern for such services (Linck, Pousttchi et al. 2006). Although there are many alternatives for modelling trust (Zimmermann 1994, Blaze, Feigenbaum et al. 1999, Agency 2001, Adams and Lloyd 2002), many security and privacy proposals lack a good understanding of the notion of trust and the use of an appropriate trust model (Karnouskos, Hondroudaki et al. 2004). Especially autonomous privacy and security control puts more pressure on traditional trust approaches, since in such environments trustworthiness of the service provider (SP) by the user should be evaluated autonomously and dynamically. Given also the limited local resources and limited connectivity of wireless devices, a tailored trust model is needed (Wang and Kranakis 2003).

Our aim in this paper is to develop a self-disclosure trust model for ubiquitous services such that it respects autonomous privacy, security and trust. The structure of the paper is as follows: in the next section, we will elaborate on the requirements conditions and boundaries of trusted computing in ubiquitous software systems. Then we present the proposed trust model followed by the experimental work showing a design of how the proposed model can be implemented in addition to a simulation study. Then we provide an analysis of collected results and discuss related work. Afterwards, we conclude the paper and provide recommendations for future work.

**REQUIREMENTS OF TRUSTED COMPUTING IN UBIQUITOUS SYSTEMS**

Recently, we have seen how the introduction of the latest technology of smart phones with GPS capabilities like iPhone, Blackberry, Android, iPads etc. led to the introduction of a set of location-based services (LBS), including road navigators. Additionally, we have seen a rapid growth of ubiquitous systems and associated mobile applications where attention has been not only given to extending current web services models, but increasingly also to making these services ubiquitous. It is clear that the design of any information system should be based on well-defined requirements. Uncertainty associated with information disclosure makes it difficult to make good disclosure decisions (Shehab, Squicciarini et al. 2012, Such, Espinosa et al. 2012, Jin, Joshi et al. 2013). In the mobile context, users are surrounded by many others who they know
The Protection Policy for Youth Online in Japan

Solving Security and Availability Challenges in Public Clouds

Negotiating Online Privacy Rights