Chapter 9
Tailoring Privacy-Aware Trustworthy Cooperating Smart Spaces for University Environments

Nicolas Liampotis
National Technical University of Athens, Greece

Pavlos Kosmides
National Technical University of Athens, Greece

Eliza Papadopoulou
Heriot-Watt University, UK

Efstathios D. Sykas
National Technical University of Athens, Greece

Nikos Kalatzis
National Technical University of Athens, Greece

Diana Bental
Heriot-Watt University, UK

Ioanna G. Roussaki
National Technical University of Athens, Greece

Nicholas Kenelm Taylor
Heriot-Watt University, UK

ABSTRACT

The more information users disclose to pervasive systems or social media, the better quality and enhanced experience they enjoy for a wider variety of personalised services. However, the privacy concerns of individuals that use such systems have dramatically risen the last years, especially after several events of massive security breaches in various computing or communication systems that have reached the news. This chapter presents the approach being employed by the SOCIETIES project to protect the privacy of sensitive user data and ensure the trustworthiness of delivered services via social and pervasive computing systems. This framework has already been designed, implemented and evaluated via real user trials engaging wide and heterogeneous user populations. In addition to the respective requirements, architecture and features discussed herewith, this chapter elaborates on the user trial that has been conducted in university settings to validate this system focusing on the privacy and trust evaluation results obtained.

DOI: 10.4018/978-1-5225-8897-9.ch009

INTRODUCTION

Latest advances in sensor technology and mobile devices have pushed forward the realisation and integration of pervasive computing (Hansmann et al., 2003; Minyi et al., 2014) in our everyday life. Sensors are embedded into objects, allowing them to obtain information from the physical world, while heterogeneous wireless networking technologies (e.g., WLAN, WiMAX, Bluetooth, LTE, UMTS, and GSM) enable sharing of information among them. Furthermore, with the advent of social media (Kaplan & Haenlein, 2010), vast amounts of personal information are being offered on a voluntary basis by the users themselves. The sensitivity of information that is disclosed, communicated and processed poses a threat to the privacy of the users, especially in cases where they are unable to fully understand and control the systems they are interacting with. These systems are responsible for providing appropriate mechanisms to ensure the protection of the privacy of their users.

It is a fact that absolute privacy can be achieved only if users do not disclose any personally identifying information. However, the pervasive computing and social networking paradigms depend on the availability of such information to provide value added services. Hence, there is a trade-off between the quality of user experience offered by these services and the preservation of user privacy. This chapter presents a privacy-enhancing framework that aims to assist users in maintaining a balance between protecting their privacy and enjoying the benefits of these technologies. This framework has been designed, implemented and evaluated within SOCIETIES, a European FP7 integrated project (http://www.ict-societies.eu), the vision of which is to transform traditional online social networks into *pervasive communities*.

A pervasive community is a group of two or more individuals who have agreed to share some of their resources, such as personal information, context data, services and devices with other members of that community. Towards the realisation of this paradigm, a set of community-centric concepts have been introduced (Doolin et al., 2012). On the one hand, a Cooperating Smart Space (CSS) represents a single participant (user or organisation) including their information and services within a distributed system of CSS nodes (user devices/cloud instances). On the other hand, a Community Interaction Space (CIS) represents and provides the interaction mechanisms for a pervasive community. CIS members interact via their own personal CSSs. The creation of a pervasive community or CIS is supported by discovering, connecting and organising relevant people and things from both physical and digital environments. This is accomplished by employing pervasive technologies, while leveraging social computing.

The usefulness of the CSS and CIS concepts has already been evaluated by three distinct user groups. One of these is the Student user group, which has been selected due to its ability to adapt to and accept new ideas and technologies. It is also the case that communication plays an important role in students' lives as social networks have become an increasingly popular communication medium. Students are also less constrained in the ways they may use a CSS compared to other users, e.g. in the Enterprise or Disaster Management domain, where the CSS must serve a clear purpose. Students can therefore utilise a wide range of novel services enabled by a CSS ecosystem that integrates information from sensors in the environment, other users or communities, as well as, social media. For example, in university living scenarios, students with similar profiles, goals or interests can discover each other to discuss topics, share study notes and meet up when they are automatically discovered to be nearby.

However, at the same time, students are concerned about managing their privacy, which has been defined as "*the right of individuals to protect their ability to selectively reveal information about themselves so as to negotiate social relationships most advantageous to them*" (EU Data Protection Directive 95/46/EC). Thus, as a minimum, the system should allow users to preserve their privacy by enabling them to