Chapter 15
Privacy and Trust Issues in Context-Aware Pervasive Computing: State-of-the-Art and Future Directions

Pierre E. Abi-Char
Institut Telecom SudParis, France

Abdallah M’hamed
Institut Telecom SudParis, France

Bachar El-Hassan
Lebanese University, Lebanon

Mounir Mokhtari
Institut Telecom SudParis, France

ABSTRACT
The growing evolution of information and communication technology (ICT) systems towards more pervasive and ubiquitous infrastructures contribute significantly to the deployment of services anywhere, at anytime and for anyone. To provide personalized services in such infrastructures, we should consider both user’s privacy and security requirements and context-awareness environment. This can be really achieved owing to context awareness systems which allow us to benefit from sensing and mobile technologies to derive more accurate data about the user and his/her location. While the availability of contextual information may introduce new threats against security and privacy, it can also be used to improve dynamic, adaptive and autonomic aspects of security, and user privacy. Moreover, context-aware information offers new opportunities for the establishment of trust relationship among involved entities (e.g., users, devices, and platforms). As context awareness represents new challenges and new opportunities regarding privacy, trust and security of users in pervasive computing environments (PCE), the main purpose of this chapter aims to survey each of the involved issues to understand and address the interdependencies among them.

DOI: 10.4018/978-1-61520-682-7.ch015
INTRODUCTION

Besides Security, Privacy and Trust in pervasive computing are currently hot issues in digital information technology area. As observed by (Saltzer & Schroeder, 1975), security is used to describe techniques that control who may use or modify private data and context information, privacy is viewed as the ability of an entity to determine whether, when, and to whom information is to be released and finally trust denotes the grounds for confidence that a system will meet its security objectives. Privacy preservation has been identified as an important factor to the success and acceptance of pervasive computing systems. The development of mobile communications technologies and ubiquitous computing paradigm and the convergence of m-healthcare, m-business, m-entertainment and m-education services have raised the urgency of dealing with privacy threats (i.e. personal information, etc.). These threats are caused by the detection of personal sensitive information such as location, preferences, and activities about individuals through sensors or invisible computing devices, gathering collating data and deriving user context, available anywhere and at any time and for anyone. Organizations and service providers collect large amounts of personal information about individuals in order to deliver suitable services to them; this could lead to a conflict between personal information owners (individuals) and information collectors (e.g. service providers) regarding privacy control. This conflict is mainly caused by the confrontation between service providers, aiming to collect more information about users in order to provide personalized services, and users’ requirements of controlling their privacy attributes. In (Cranor, Reagle & Ackerman, 1999) it is mentioned that people dislike automatic transfer of identifiable and personal data, especially when information is spread to other entities beyond their control.

Context-aware computing environments may use information provided by many sensors to acquire knowledge about the users’ context. These sensors can be invisible to users who consider the act of gathering information about them without being notified as a great threat to their privacy. If the risks of privacy violation when using a context-aware application can not be estimated, users may be unwilling to use such systems. This is why privacy control is essential to be integrated in the design of any new context-aware computing platform. However, the quests for authentication, access control, and user privacy protection conflict with each other in many aspects and the problem is highly complex as the context information of users is more of a concern. On one hand, service providers want to authenticate legitimate users and make sure they are accessing their authorized services in a legal way. On the other hand, users want to maintain the necessary privacy without being tracked down for wherever they are and whatever they are doing. Furthermore, new provided services generally depend on the user identity information, context-awareness information and corresponding pre-established and context-aware dynamically evaluated trust relationship to accomplish user privacy and authentication and to conduct access control. The tradeoff between privacy and authentication poses great challenges to security designers. This is why the conflict between user privacy protection and user authentication process makes security design in Pervasive Computing Environments (PCE) a very challenging task.

The rest of the chapter is organized as below. We firstly introduce the features, security challenges and requirements of pervasive computing. Then, we give an overview of context-aware computing. Furthermore, the privacy issue is discussed, followed by the trust researches in pervasive computing. In addition, we specify the requirements of achieving authentication in the PCE, especially for supporting context awareness and privacy. Finally we review the related work conducted in this area and conclude the chapter by proposing a number of future directions.