Chapter XIII
Privacy Automation in Context–Aware Services

Amr Ali Eldin
Accenture, The Netherlands

Semir Daskapan
Delft University of Technology, The Netherlands

Jan van den Berg
Delft University of Technology, The Netherlands

ABSTRACT

With the growing interest in context-aware services, attention has been given to privacy and trust issues. Context-aware privacy architectures are usually proposed and developed without taking into account the trustworthiness of a service provider. Therefore, this chapter deals with two challenges in context-aware services. The first one is to improve privacy architectures with a trust functionality and the second one is to integrate this refined privacy architecture in larger service-oriented architectures (SOAs).

INTRODUCTION AND BACKGROUND

With the rapid developments of mobile telecommunications technology over the last two decades, a new computing paradigm known as anywhere and anytime or ubiquitous computing has evolved. Consequently, attention has been given not only to extending current (mobile) web services models, but increasingly also to make these services context-aware. Despite the expected benefits behind this new technology and the need for developing more and more context-aware applications, we enunciate that privacy and trust represent challenges for the success and widespread adoption of these services (Amr Ali Eldin & Stojanovic, 2007).

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.
Privacy has always been of the utmost importance to people since Warren and Brandeis (1890) who wrote “The Right to Privacy” in response to an article that contained personal information about the Warren family. There has been an intensive concern about privacy threats and ways of protecting user privacy in the literature. Privacy threats arise from the linkage between users’ identity and their private information. Simply, it can be seen that breaking this link helps protecting users’ privacy. This can be achieved by either protecting user identity as in most anonymity and pseudonymity solutions (Beresford & Stajano, 2003; Chaum, 1985; Lysyanskaya, Rivest, Sahai, & Wolf, 1999; Wang, 2004) or by controlling private information collection. Most literature focused on the assumption that unknown service providers are simply non-trustworthy and the traditional approach to privacy was always to block all un-authorized requests to private information using access control mechanisms and anonymity solutions (Clifton, Kantarcioglu, Vaidya, Lin, & Zhu, 2002; Linn, 2005; Park & Sandhu, 2002; Sandhu, Coyne, Feinstein, & Youman, 1996; Tolone, Ahn, Pai, & Hong, 2005). Therefore, cryptographic solutions such as public key and symmetric key encryption mechanisms were always positioned as means of privacy protection. For example, a watermarking algorithm is proposed in (Agrawal & Kiernan, 2002) to encrypt database records by a user’s private keys. To make these records usable by others, a user’s private key has to be communicated so again an assumption has to be made on trustworthiness. Further, real identities can be leaked still when engaged in an online transaction by traffic analyzers (Christian Hauser, 2002; Christian Hauser & Kabatnik, 2001; Linn, 2005).

In analogous to the previous efforts, we cannot guarantee an ultimate privacy. In daily life interactions we need to make assumptions of a service provider (SP) trustworthiness to some degree. Based on this trustworthiness degree, an SP might be given a certain type of access to sensitive information. This is called the authorization or informed consent decision. The tolerance of non-trustworthy service providers seems, however, to be non-realistic in daily life interactions with increasing mobile services (Daskapan, Vree, & Ali Eldin, 2003). Given the fact that many proposed privacy architectures are developed without the clearance of this trust issue, the purpose of this chapter is to propose an integrated solution to privacy that automates trustworthiness assessment as well.

The chapter is organized as follows. In the next section we elaborate in details on the research problem and related work. Then, we introduce the extended ShEM architecture concepts and components where we extend its architecture to introduce a trust valuation mechanism and its high level architecture showing how it is integrated in ShEM overall architecture. Then we develop the high level design of the overall architecture and apply it in a case using the service-oriented architecture (SOA) approach. Finally, we conclude the chapter highlighting potential future work.

**PROBLEM DESCRIPTION AND RELATED WORK**

In this section, we discuss the motivation behind this work and the type of research problem we are addressing. The research problem investigated in this work can be seen as a multidisciplinary problem where legal, social and technical domains are concerned with providing solutions. In this work, we focus on the technological perspective taking into consideration requirements set by the other domains.

There is a trade-off between users’ privacy needs and their motivation behind giving private information away. Complete privacy is impossible in a society where a user would have to interact with other members of the society such as colleagues, friends, or family members. Each flow of user information would reveal some private
Related Content

Comprehensive Structure of Novel Voice Priority Queue Scheduling System Model for VoIP Over WLANs
[www.igi-global.com/article/comprehensive-structure-novel-voice-priority/66065?camid=4v1a](www.igi-global.com/article/comprehensive-structure-novel-voice-priority/66065?camid=4v1a)

Ambient Intelligence
[www.igi-global.com/chapter/ambient-intelligence/37781?camid=4v1a](www.igi-global.com/chapter/ambient-intelligence/37781?camid=4v1a)

Research on Parts Measurement Method Based on Machine Vision
[www.igi-global.com/article/research-on-parts-measurement-method-based-on-machine-vision/100437?camid=4v1a](www.igi-global.com/article/research-on-parts-measurement-method-based-on-machine-vision/100437?camid=4v1a)

Interactive Books in Augmented Reality for Mobile Devices: A Case Study in the Learning of Geometric Figures
[www.igi-global.com/chapter/interactive-books-in-augmented-reality-for-mobile-devices/92931?camid=4v1a](www.igi-global.com/chapter/interactive-books-in-augmented-reality-for-mobile-devices/92931?camid=4v1a)