Chapter 13

A Privacy Service for Comparison of Privacy and Trust Policies within SOA

David S. Allison
The University of Western Ontario, Canada

Hany F. EL Yamany
Suez Canal University, Egypt

Miriam A. M. Capretz
The University of Western Ontario, Canada

ABSTRACT

Privacy for Service-Oriented Architecture (SOA) is required to gain the trust of those who would use the technology. Through the use of an independent Privacy Service (PS), the privacy policies of a service consumer and provider can be compared to create an agreed upon privacy contract. In this chapter, the authors further define a metamodel for privacy policy creation and comparison. A trust element is developed as an additional criterion for a privacy policy. The authors define the PS, outline what operations it must perform to accomplish its goals, and present how the PS operates in different scenarios. They believe the PS, combined with the enhanced metamodel, provides a strong solution for providing privacy in an SOA environment.

INTRODUCTION

The definition of privacy continues to evolve along with the times it inhabits. In 1888, Justice Thomas M. Cooley famously defined privacy as “the right to be left alone” (Cooley, 1888). Almost a hundred years later, privacy was viewed as the ability to control the release of information about oneself (Parent, 1983). In the digital world of the 21st century, releasing information about ourselves is often a necessity of communication, which is done in many cases without our knowledge. For this reason, we extend the definition of privacy to include not only the ability to control information about ourselves that has not been released, but to also retain some measure of control over the information that has.

DOI: 10.4018/978-1-4666-0978-5.ch013
Service-Oriented Architecture (SOA) offers the policies, practices and frameworks required to provide and consume services (Sprott & Wilkes, 2004). SOA provides a solution to finding, utilizing and integrating many different services to meet the business requirements of a consumer. The usefulness of services in providing business solutions is directly linked to the amount of interactions that exist between different services. This property of services poses a challenging problem for dealing with privacy protection. As an increasing number of services are composed together, often from multiple parties, it becomes easier for a consumer to unwittingly expose private information. A common approach to protecting consumers from this exposure is to provide pseudonyms to identifying information. However this solution is incomplete as even hidden identities can be deduced by tracking patterns of usage (Kanneganti & Chodavarapu, 2008). As services can provide complex and confidential actions such as Internet banking (Shan & Hua, 2006) and business-to-business (B2B) commerce (Vitvar et al., 2007), the protection of consumer data is of the utmost importance.

A privacy policy allows both the service consumer and provider to outline their preferences and concerns pertaining to their private data. We describe an expansion to our previously defined metamodel (Allison, EL Yamany, & Capretz, 2009) that will provide the consumer with greater input into how their data is used. This will be done through the introduction of a trust element to give the consumer a measure of control over the Privacy Service (PS) which acts as the negotiator of a privacy contract. The PS uses specific operations to compare the privacy policies of a service consumer and provider.

When discussing the entire security of SOA, privacy is often one of the smallest aspects highlighted (Kanneganti & Chodavarapu, 2008; Nakamura et al., 2005). Due to this, it is important to examine privacy both in and out of an SOA environment. In this chapter relative works are discussed which deal with privacy and trust issues. These works provide insightful comparisons to the research presented in this chapter.

This chapter will also present an outline of how privacy elements are selected to create a comprehensive SOA privacy solution. These elements outline what each party, the consumer and provider, are comfortable with providing to each other in a privacy contract. Together these elements create a privacy metamodel consisting of six elements: collector, what, purpose, retention, recipient and trust.

The sixth element, trust, is presented in greater detail. The addition of trust to the selection of privacy elements emboldens the consumer with a degree of control over what PS oversees the negotiation of their privacy contract. Without this ability, the consumer would have nothing to ensure themselves that the policy comparison is completed without bias.

Furthermore, this chapter will illustrate each of the elements that together create privacy rules, including the element of trust. It will be explained why the element trust is required, and how trust is defined. A Privacy Service will also be introduced to be used as a third party between the service consumer and provider. The Privacy Service will be outlined and the operations it can perform will be explained.

Finally, this chapter will present a proof of concept to outline how the Privacy Service performs and the interactions it creates in different scenarios.

At the end of this chapter, we will introduce some scenarios for establishing the interactions among the described services within an SOA security framework in order to provide the sufficient and necessary security dimensions for an SOA environment.