Chapter 10
Consumer Privacy Enforcement in Context-Aware Web Services

Georgia M. Kapitsaki
University of Cyprus, Cyprus

ABSTRACT

Privacy protection constitutes a genuine human right reflected both in the legislation and in different aspects of software engineering. Sensitive information needs to be protected in end-users interaction with Web Services especially in cases, where context-aware features are included. In this work the authors address the inclusion of consumer privacy preferences in the provision of context-aware Web Services. To achieve this the authors propose, on the one hand, a preferences language, where end-users can specify their privacy options, namely Consumer Privacy Language, and, on the other hand, a seamless enforcement mechanism that considers consumer preferences by intercepting and modifying appropriately Simple Object Access Protocol request and response messages. The enforcement approach has been evaluated based on various execution metrics for an example use case consisting of various Web Services and for different user configurations demonstrating the usefulness of the approach assisting towards the provision of privacy-aware environments.

INTRODUCTION

Sensitive information is all around us nowadays distributed and spread at a large scale in different ways and under different conditions strengthened through the use of smartphones and online or mobile social networks. Although contradictory the collection and exploitation of this information is a desirable feature of various applications that take it into account in order to make appropriate adaptations of services and applications to user and service surroundings. This characteristic is referred to as context-awareness and is linked with the collection and use of data either through device embedded sensors (e.g., accelerometer, temperature sensor), sensors in the user environments (e.g., RFIDs) or requests to remote locations including Web Services (WSs).

These market trends call for the development of technologies that enable service providers to manage sensitive information in an adequate manner, attending to laws by reducing the risk of contravening legislation, forming part of Privacy Enhancing Technologies (PETs). Privacy has

DOI: 10.4018/978-1-4666-8111-8.ch010

broad historical roots: Aristotle made a distinction between the public sphere of political activity and the private sphere associated with domestic life, whereas in the Harvard Law Review paper by Warren and Brandeis (1890) privacy is described as "the right to be let alone." Many definitions have been given for privacy and these have evolved over the years through the introduction of information and communication privacy. Nowadays the right to privacy is a permanent and genuine right of any person. The Privacy Rights Clearinghouse (PRC), a non-profit organization dedicated to protecting the privacy of American consumers, indicates Internet privacy threats, data profiling and wireless communications and location tracking among the current privacy threats. The importance of privacy is also reflected in the legislation. The first influential text was the United States Privacy Act (United States, 1974) adopted by the Congress in 1974, whereas recently in 2012 the European Commission proposed a General Data Protection Regulation amending Directive 95/46/EC (European Commission, 2012).

In this work we view privacy as "the ability of individual's control over the use and dissemination of sensitive information," where the term sensitive is subjective. When interacting in Service-Oriented Computing (SOC) environments, end-users or consumers may provide different kind of information ranging from personal data (e.g., occupation, age) to transactional information (e.g. ID number, credit card information). The disclosure of such data may bring smaller or bigger problems to the end-user leading even to falsified transactions, when security guarantees are not provided.

Web Services related to context – as either requesters or providers of context information – are relevant, when sensitive data is considered, especially through their ability to be consumed in different environments. Many Web Services are stateless in the sense that they do not store the state of the session with the user. A request is made and a response is sent back. Nevertheless, there is no guarantee that information present in user requests is not stored for future use, statistical or advertisement purposes. It may also be the case that a service invokes a third party without the user's prior knowledge. Some internet sites include information for such cases: *Our Web sites may include links to third party Web service providers who may collect personal data* (Data Service & Information).

The provider and the consumer of the WS often have different preferences regarding the available choices of features and parameters linked with the service interaction. In this paper we focus on the one side of the privacy coin by proposing solutions to two main problems:

1. The specification of end-user preferences in context-aware WS environments, and
2. The proper integration in the Web Service provision chain.

For the former we present a policy language that reflects user preferences. Although several privacy policy models have been proposed, e.g., XACML, EPAL, they do not focus both on privacy and onSOC. Indeed it is probably practically impossible to create a universal language applicable in all domains (Kumaraguru, Cranor et al. 2007). Moreover, none of the existing approaches considers the dimension of context or reaches to the end-user of the WS: that is the person accessing a WS or a chain of WSs; the available solutions are rather applied on a lower level expecting interaction among peers (consumer, provider interaction). For instance the first version of Platform for Privacy Preferences (P3P) was initiated by W3C with the aim to express website privacy policies in machine-readable format. Regarding the integration in WS invocation a mechanism for reflecting consumer privacy needs in context-aware WSs on runtime is proposed. This mechanism extends our previous work on context-aware WSs that relies on message interception (Kapitsaki, Kateros et