Chapter 69
Context and End-User Privacy Policies in Web Service-Based Applications

Georgia M. Kapitsaki
University of Cyprus, Cyprus

ABSTRACT

Privacy protection plays a vital role in pervasive and web environments, where users contact applications and services that may require access to their sensitive data. The current legislation, such as the recent European General Data Protection Regulation, is putting more emphasis on user protection and on placing users in the center of privacy choices. SOAP (simple object access protocol)-based and RESTful services may require access to sensitive data for their proper functioning, but users should be able to express their preferences on what should and should not be accessed. In this chapter, the above issues are discussed and a solution is presented for reconciling user preferences expressed in privacy policies and the service data needs tailored to SOAP-based services. A use example is provided and the main open issues providing directions for future research are discussed.

INTRODUCTION

Sensitive data may be used in different applications and it is important to make sure that they cannot uniquely identify a person, as this may pose a danger for her private sphere. Sensors in mobile devices can be accessed both by native application code and by cross-platform applications that use features of HTML5, e.g. geolocation, battery status, network information, device motion and orientation. Other sensitive data may be returned when invoking web services that contain information of this nature (e.g. location, weather services).

At the same time web services are considered as building blocks of larger applications and are used in different environments, from mobile and pervasive computing to cloud and web applications leading to web-service based applications (Georgantas, 2018). Many such applications require user data in order to function properly or offer a personalized used experience. Some services provide even context-aware

DOI: 10.4018/978-1-7998-8954-0.ch069

capabilities, when the user environment or context is considered in order to adapt the service to user needs. Therefore, utilizing user data is in many cases desirable, in order to make appropriate adaptations of services and applications to user surroundings. Examples of such context elements can be found in the user location, current or past activities, health and weather conditions. There are different solutions that allow context acquisition by using the aforementioned HTML5 APIs, accessing device sensors with platform-specific code or using different kinds of services (Lee et al., 2015).

Importance to privacy has also been given by legislation. The Health Insurance Portability and Accountability Act (HIPAA) (Boyce, 2017), the Act on the Protection of Personal Information (APPI) (Adams, 2009) and the recent European General Data Protection Regulation (GDPR) (Voss, 2017) put a lot of emphasis on user privacy and on placing user in the center of the decision process of how her personal data will be handled (Kolter, 2010). There recent advances call for mechanisms and technologies that enable web services and service-based applications to be privacy-aware considering user's view, by reducing the risk of contravening legislation, forming part of Privacy Enhancing Technologies (PETs).

In the framework of this chapter, privacy is viewed as "the ability of individual's control over the use and dissemination of sensitive information", where the term sensitive is subjective. 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 marketing purposes.

Having as motivation the above, in this chapter the user view is targeted. It is described how user preferences can be captured and considered in the invocation of web services, especially for the case, when these web services request access to context information in order to function properly. They may be able to retrieve this information from different sources, but in many cases other web services can also be utilized. Specifically, the work presented formulates end-user preferences in context-aware web service-based applications and these preferences are subsequently combined with adaptation during web service invocation. Nevertheless, the service provider side is also important and mechanisms that reconcile the views of the two sides, i.e. user and provider, are also required.

The user preferences and the web service invocation mechanism can be found in previous publications (Kapitsaki, 2013a; Kapitsaki, 2013b). This chapter outlines the content of the user privacy preferences providing extensions to the original content captured in Consumer Privacy Language version 2.0 (CPL-2.0). It also provides the structure of the management architecture for SOAP (Simple Object Access Protocol)-based services extending a previous message interception approach (Kapitsaki et al. 2008). How other types of environments (i.e. RESTful services) can be considered for message interception and adaptation is also discussed. Finally, it builds on recent advances in the field discussing open research directions offering thus, a current view of privacy protection for web service-based applications that require user context.

The rest of the text is structured as follows. The next section presents background information focusing on related works on web service descriptions, privacy policies and web service privacy protection mechanisms. The section that comes next is dedicated to how user preferences can be expressed with semantics focusing on the end-user side, whereas afterwards it is presented how SOAP-based web services can consider user preferences when requesting context information. A demonstration of an example use case and a presentation of open issues follow. The final section concludes the text.