

A Privacy Framework for Composite Web Services

Ibrahim M. Al-Nedhami
Dept. of Computer Science
University of Pune
Ibrahim@cs.unipune.ernet.in

Pradeep K. Sinha
Center for Development of
Advanced Computing (C-DAC)
Pune University Campus
psinha@cdac.in

Abstract

The growing number of services offered on the web has led to increasing interest in the area of composing web services by including several existing web services to achieve new and more useful services. However, composing new web services from existing web services to obtain new functionality for business-to-business and business-to-consumer applications has raised privacy concerns. We have proposed a framework that addresses consumer privacy concerns in composite web services. Our framework provides a technique for privacy policy checking between a consumer and a service provider for compatible privacy policies. For tracking of consumer's personal information, we propose a technique to let the consumer access all web service transactions carried out in a composite web service.

Keywords

Web Service Composition, Composite Web Services, Privacy Framework, Consumer Privacy Concern, Service Oriented Computing

1. Introduction

Web services have become an important means of interaction between consumers and service providers for online business services and solutions. A *web service* is a software application that provides business functionality or information to other applications through an Internet connection using different XML-based languages such as Universal Description Discovery and Integration (UDDI) [1], Web Services Description Language (WSDL) [2], and Simple Object Access Protocol (SOAP) [3]. These web languages are designed to define standards for service discovery, description, and messaging protocols. These web services standards do not provide the facility of dynamic service composition. *Service composition* is described as the process of creating customized services from existing services by a process of dynamic discovery, integration and execution of those services in deliberate order to satisfy a request from consumer [4]. A service composed in this manner is called a *composite web service*. Composite web services enable many heterogeneous applications to interconnect and work together without having to spend much time configuring the environment to allow applications to communicate effectively. A composite web service, therefore, uses one or more web services to process a web service transaction (WS-transaction). To complete the WS-transaction's goal, each web service takes care of its own part of the total service required by the WS-transaction.

There are many standard languages proposed to represent web service composition like BPEL4WS [5] and WSCI [6]. In current specifications and standards, a consumer who requests a service becomes vulnerable to misuse of his/her personal information by the service provider or a third party. The consumer does not have enough control after submitting his/her personal information to the service provider. He/she does not know how the service provider will use his/her personal information, to whom

all will the service provider send the information, and who will keep the information for how much period. Hence, privacy of personal information becomes a critical issue in composite web services. This paper proposes a framework that allows a consumer to be confident of his/her personal information privacy while communicating with a composite web service. The framework also allows the consumer to track all WS-transactions pertaining to his/her personal information.

The paper is organized as follows. Section 2 provides an overview of the proposed framework and explains the roles of its various components. Section 3 illustrates our approach with an example scenario and provides algorithms for Privacy Policy Control and Transaction Tracking & Registration. Section 4 defines standard for recording contracts and information transfers to ensure a more consistent approach of information exchange. Section 5 provides the justification for the composition language used by us to write composite code in our prototype implementation. Section 6 compares our proposed framework with other trust building frameworks in the literature for composite web services. Finally, Section 7 concludes the paper with a summary of key features of our proposed privacy framework for composite web services.

2. Framework Overview

Figure 1 shows the architecture of our proposed framework for composite web services, which consists of the following major components: a) Composite Web Service Management, b) Service Provider Privacy Model, c) Consumer Privacy Model, d) Privacy Policy Control, e) Transaction Tracking & Registration, f) Service Provider Enforcement, and g) Consumer Enforcement.

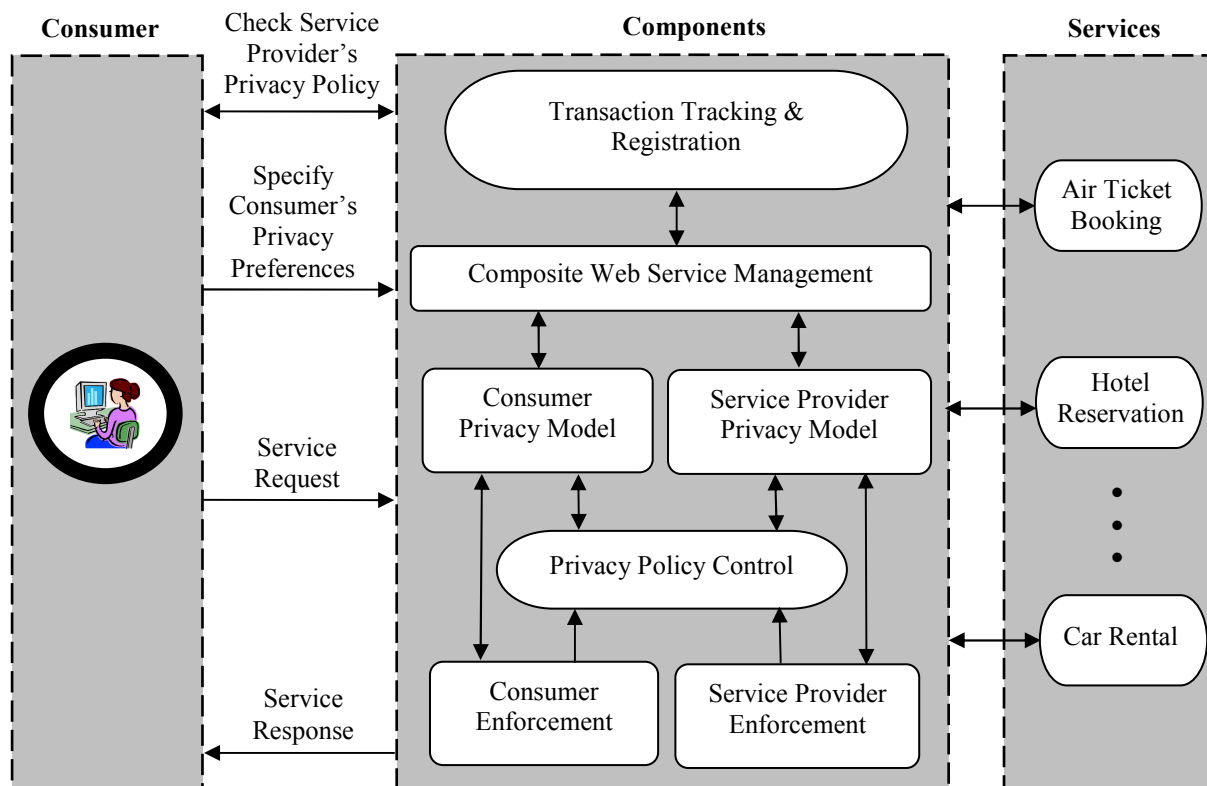


Figure 1: Proposed framework architecture for composite web services.

The component services are shown in the right part of the figure. Each component service accepts inputs from its caller, and then interacts with other entities such as web sites or web services, and returns requested results to the caller. These services are glued together using the composition code, resulting in a composite service, which typically provides richer functionalities. Consumers can express their privacy concerns using Consumer Privacy Model. These policies capture what types of consumer data they are willing to share with which service providers. When a consumer interacts with a composite web service, he/she first requests the Service Provider Privacy Model and checks whether the model is compatible with his/her privacy policies. If compatible, the service request is forwarded to the service provider. Otherwise, the consumer can either relax his/her privacy policy to use the service, or present his/her privacy policy as an obligation to the service provider. For example, if an Internet shopping service provider needs consumer's email-ID to offer its service, the consumer may agree to reveal his/her email-ID to obtain the service, or may refuse to reveal his/her email-ID and present this violation as an obligation to the service provider to see if the service provider can still provide the service. The service provider may still be able to provide most of its services, e.g. provide price quotes from those merchants, which do not ask for email-ID. Hence, in our approach, compatibility violations between a Service Provider Privacy Model and a Consumer Privacy Model are used to either guide the consumer to relax his/her policies, or to automatically generate obligations to be satisfied by the web service. Our approach also involves tracking, and recording of flow of information to and from the component web services, and within the composite service, as and when it happens.

Wei Xu et al. [7] proposed the use of data labels based on sensitivity levels and information categories. We use two attributes, sensitivity level and information category, to classify user's data into many levels to ease policy specification and management. For example, sensitivity levels can be level-1, level-2 and level-3, and one might consider his/her credit card number and bank account number to be of level-1, the credit card expiration date and the bank name to be of level-2, and data such as country of level-3. Data items can also be categorized into different information categories such as personal information, financial information, health information and address information. Using the attributes sensitivity level and information category, a consumer can specify more expressive privacy policies. Hence, when a consumer decides to release the information to different web sites or web services, he/she can put his/her trust levels for web services or web sites as high trust, medium trust and low trust. Figure 2 presents example data labels based on sensitivity levels and information categories.

Information Categories	Sensitivity Levels of Information		
	Level-1	Level-2	Level-3
Personal Information	SSN	age	name, gender
Health Information	medical history	blood pressure	eye's color, weight
Financial Information	account no.	bank branch	bank name
Address Information	apt. no.	street no.	city, zip code, state, country
Payment Information	CC no.	CC exp. date	CC type

SSN – Social Security Number
 CC – Credit Card

Figure 2: Information categories and sensitivity levels

Roles of the various components of the proposed framework are as follows:

1. **Service Provider Privacy Model:** A service provider can express its privacy policy using the Service Provider Privacy Model. These policies deal with:
 - What information will a service provider collect from a consumer
 - How will the service provider use consumer's information
 - With whom will the service provider share the consumer's information
 - How can the consumer access his/her information
 - For how much time will the service provider save the information
 - How will the service provider protect the consumer's information
2. **Consumer Privacy Model:** A consumer can specify his/her privacy preferences using the Consumer Privacy Model. A consumer's privacy preferences include his/her choices such as which information will he/she like to disclose to whom, and which information will he/she not like to disclose.
3. **Privacy Policy Control:** It validates a consumer's privacy preferences and a service provider's privacy policy for compatibility. If compatible, the consumer is allowed to use the service, else the consumer is asked to change his/her privacy preferences.
4. **Service Provider Enforcement:** When a consumer's privacy preferences and the service provider's privacy policy do not comply fully, the Service Provider Enforcement checks with Service Provider Privacy Model if the service provider can provide alternate attributes. For example, the service provider of an airline ticket booking service requests mobile no. from the consumer, but if he/she doesn't agree, then an alternate choice can be provided to the consumer (e.g. email-ID instead of mobile no.).
5. **Consumer Enforcement:** When a consumer's privacy preferences and the service provider's privacy policy do not comply fully, the Consumer Enforcement checks with Consumer Privacy Model, if the consumer is willing to relax its privacy preferences.
6. **Transaction Tracking & Registration:** It records and tracks all WS-transactions between a consumer and a service provider, and gives alert to the consumer's email-ID when a WS-transaction happens, including the agreement done between the consumer and the service provider. For example, when the composite service submits some personal information of a consumer that is required by a service provider of airline ticket booking service, then one copy of that WS-transaction is sent to Transaction Tracking & Registration unit. Later, if a third party requests some personal information from the web service (second party), same recording will happen for the WS-transaction.
7. **Services:** Services are grouped together using composition code to form a composite web service. The services grouped together perform different functions to help consumers meet their multiple associated requirements. For example, multiple associated requirements of a travel arrangement such as Air ticket booking, Hotel reservation, and Car rental can be part of a composite web service.
8. **Composite Web Service Management:** It is an interface between consumers' requests and web services. It includes business logic for interaction among the various components of the composite web service.

3. An Example Scenario

We illustrate our approach with an example of a travel arrangement service, which is composed of three services: Airline ticket booking service, Hotel reservation service, and Car rental service. Clients (consumers) can make their travel arrangement requests to a single service provider, which is a composite web service. To get a travel arrangement request serviced, a client checks the privacy policy of the composite web service and then creates his/her privacy preferences. After the client submits his/her privacy preferences, Privacy Policy Control unit checks privacy policy compatibility between the client and the composite web service (service provider). If there is no compatibility between the two, service provider enforcement or consumer enforcement is created. When both are compatible, copy of agreement recorded is sent to Transaction Tracking & Registration, and then the Composite Web Service Management unit invokes the three services to get the travel arrangement request processed.

Algorithm 1: Privacy Policy Control

Privacy Policy Control algorithm describes how the privacy preference of a consumer is found/made compatible with the service provider's privacy policy. The pseudocode for the algorithm is given below. In Lines 1&2, two arrays are read, which include privacy policy of service provider (e.g. credit card no., email-ID, date of birth and mobile no.) and privacy preferences of consumer (e.g. credit card no., date of birth, mobile no. and email-ID). In Lines 4&5, one or more attributes of privacy policy of service provider and privacy preference of consumer are selected for comparison (e.g. mobile no.). If they are compatible (consumer agrees to the required privacy policy of the service provider), then in Line 6 that attribute is saved as compatible between them. Otherwise, in Line 8 the service provider sends alternative attribute to the consumer (e.g. email-ID). If consumer does not agree for alternative attribute, then in Line 12 it asks the service provider for enforcement. Line 16 saves matching attribute in matching list when the service provider agrees to relax the privacy policy in Line 15. In Line 18, the service provider sends obligation to the consumer if submission of one of the attributes (e.g. mobile no. or email-ID) is mandatory to provide the service.

```
1: Input: = list of privacy policy of service provider (PPOSP)
2: Input: = list of privacy preferences of consumer (PPOC)
3: Begin
4:   Select (PPOSP) & (PPOC) from list
5:   If (PPOSP = PPOC) then
6:     Record it as a matching point in the contract
7:   Else
8:     Send alternative point to consumer
9:     If (The consumer agrees for alternative point) then
10:      Record it as a matching point in the contract
11:    Else
12:      Request the composite web service (service provider) for enforcement
13:    End if
14:  End if
15:  If (service provider agrees) then
16:    Record it as a matching point in the contract
17:  Else
18:    Send obligation to consumer
19:  End if
20: End
```

Algorithm 2: Transaction Tracking & Registration

Transaction Tracking & Registration algorithm describes how a WS-transaction is recorded when a consumer submits his/her personal information to a web service (service provider) or the web service sends that information to a third party (business-to-business). The pseudocode for the algorithm is given below. In Line 1, consumer's request is read (e.g. airline ticket booking request). In Line 3, a suitable service provider is selected to provide the requested web service. Personal information (e.g. SSN, CC. no. and address) of the consumer is sent to the service provider in Line 5 and the consumer is intimated about it in Line 6 if the service provider requires consumer's personal information in Line 4 for offering its service. At the same time, one copy of that information is sent to Transaction Tracking & Registration unit including the WS-transaction no., date and time. Similar copy of consumer's information along with the third party web service provider no. is sent in Line 11 to Transaction Tracking & Registration unit according to the contract, if there is a need to share the consumer's information with a third party web service provider to complete the service requested by the consumer in Line 10.

```

1: Input: = Consumer's request
2: Begin
3:   Select suitable service provider to invoke the consumer's request
4:   If (service provider requires some personal information of the consumer) then
5:     Send the personal information to the service provider
6:     Send alert to the consumer intimating personal information has been sent to the
       service provider
7:     Send copy of WS-transaction number and contract number to
       Transaction Tracking & Registration unit
8:     Send response to the consumer when the service is completed
9:   End if
10:  If (third party needs to share the information of the consumer) then
11:    Send copy of WS-transaction number, contract number, time, date and
       number of service provider that received personal information of the consumer
       to Transaction Tracking & Registration unit
12:  End if
13: End

```

4. Contracts and Information Transfers

The centralization of control in the Transaction Tracking & Registration unit requires some standardization of the manner in which contracts and transfers are recorded to ensure a more consistent approach of information exchange. We use the standard information shown in Figure 3 and Figure 4, which was proposed in [12].

Contract no.	Consumer no.	Service Provider no.	Start Date	End Date	Information Descriptor

Figure 3: Standard for recording a contract between a consumer and a service provider

Having a unique number for each contract, consumer, and service provider is critical to the management of contracts. The start date and end date indicate the period for which consent has been given. In addition to contracts, every information transfer between a consumer and a service provider as per an agreed

contract also needs to be standardized. Figure 4 shows the standard used for linking information transfers to the consent contract that authorized them to exchange information.

Transfer no.	Contract no.	Service Provider no.	Information Descriptor

Figure 4: Standard for recording an information transfer between a consumer and a service provider as per an agreed contract.

Having a unique number to identify the transfer and service provider receiving the information is critical to the management of information transfers. The contract no. identifies the relevant contract. The Information Descriptors of Figures 3 and 4 must match or the one in Figure 3 must be a superset of the one in Figure 4. The standardization of information in this fashion enables the Transaction Tracking & Registration unit to provide a consistent interface and summary across all contracts and transfers for a given consumer. This makes it easy for the consumer to follow the flow of his/her personal information in a business process network.

5. Composition Language

Several standard languages have been proposed for web services composition, such as BPEL4WS [5] and WSCI [6]. We used NuSOAP [13], which is a powerful API developed for PHP platform, to write composite code in our prototype implementation. One of the key features of NuSOAP is the built-in WSDL support. The required libraries are contained in a file called *nusoap.php*.

As a prototype implementation of our framework, we implemented a travel management service. The inputs to this service are the origin and destination of travel; number of seats; and departure date and time. Composite web service is built for searching a number of leading airline web services, whose results are put together in a consistent order for the user to choose the most ideal itinerary. After the consumer chooses a web service (e.g. airline-1) and submits his/her request, based on compatibility between privacy preferences of the consumer and privacy policy of the chosen web service, the consumer's request is allowed/denied processing. Thus, the privacy of the consumer and the details of his/her travel are preserved appropriately.

6. Comparison with Related Work

Various types of trust building frameworks have been described in the literature for composite web services. Wei Xu et al. [7] proposed a mechanism to address consumer privacy concerns. It provides techniques for checking the models at a consumer's site for compliance with the consumer privacy policies. If there is policy violation, the framework generates obligations for the composite web service. However, in our framework, checking the policy preferences of the consumer and policy of the composite web service to find the differences between them is done first, and then the composite web service is requested to provide alternate attributes, if the consumer does not agree to disclose some of his/her personal information attributes. Our framework also provides policy tracking and registration of WS-transactions. A consumer can track all WS-transactions that happened for his/her personal information by date, time, and target service providers.

In semantic web, some researchers who consider protecting personal information such as in [8], proposed a semantic-based privacy framework for web service that allows user agents to automatically negotiate with web services on the amount of personal information they will disclose. In this framework, key

privacy is considered from two aspects: relieving of minimal information about a user and limited user interaction. The framework also lets web services declare their input parameters related to user's personal information in two ways: Mandatory or Optional. If a user does not want to give some mandatory input to a web service, then the web service declares alternate data elements. The framework uses DAML-S, which defines an upper ontology for describing semantic web services. However, the framework does not present the facility for the consumer to track all WS-transactions through policy tracking and registration of WS-transactions [8]. On the other hand, there are a few research work in this area, which are related to credential based access control technique. For example in [9], Rezgui et. al proposed an approach for preserving privacy in government web services through personal information stored and retrieved from a database and preventing unauthorized access to information by credential based access control technique. Also they view privacy in web services from aspects of user privacy, data privacy, and service privacy. They do not allow tracking of personal information when a consumer releases it [9].

The Platform for Privacy Preferences (P3P) [10] is a protocol that works automatically through user agent (web browser) to negotiate with a web site. It compares the privacy policy of the web site with user preferences and then the appropriate action is taken. If data collection is acceptable according to user preferences, the page displays, otherwise the user gets an alert by a warning message about P3P policy content, and then the user is given the choice between continuing the action or canceling it [10, 11]. P3P has some problems. It is not designed to eliminate or reduce the exchange of personal data, and it does not provide any mechanism to ensure that web sites act according to their privacy policies. Moreover, P3P protects the privacy of individual web sites and is not suitable for composite web services.

Liam and Max [12] proposed the concept of an "information transfer registry" as a mechanism to track compliance in business-to-business network. This registry keeps a record of all information transfers. However, the mechanism does not check the compatibility between consumer policy preferences and service provider privacy policy before executing transfer of personal information. Also, there is no negotiation between both sides.

7. Conclusion

The proposed personal information control mechanism provides high accountability and transparency to consumers. The proposed framework enables preserving of privacy in composite web services. A consumer can request the privacy policy of a composite web service and can specify his/her privacy preferences. The privacy checking policy of the framework compares the privacy policies of both sides for compatibilities between the consumer privacy policy and the privacy policy of the composite web service. If compatible, it forwards the request to the composite web service to invoke the service, otherwise it requests the composite web service for privacy policy enforcement. If enforcement is not possible, it gives obligation to the consumer, and then the consumer decides for enforcement to get the service, or searches for any other composite web service compatible with his/her privacy preferences.

8. References

- [1] "Universal Description Discovery and Integration (UDDI), UDDI Version 3.0," UDDI Spec Technical Committee Specification, 19 July 2002. Available from: www.uddi.org/pubs/uddi-v3.00-published-20020719.htm
- [2] "Web Services Description Language (WSDL), Version 1.2," W3C Working Draft, 9 July 2002. Available from: www.w3.org/TR/2002/WD-wsdl12-20020709/

- [3] World Wide Web Consortium (W3C). "SOAP Version 1.2 Part 1: Messaging Framework" Available from: www.w3.org/TR/2003/PR-soap12-part-20030507/
- [4] Chakraborty, D., Perich, F., Joshi, A., Finin, T. and Yesha, Y. (2002): "A Reactive Service Composition Architecture for Pervasive Computing Environments," In 7th Personal Wireless Communications Conference (PWC 2002), Singapore, October.
- [5] F. Curbera et al. "Business Process Execution Language for Web Services," Technical Report, IBM Developer-works, 2002.
- [6] A. Arkin et al. "Web Services Choreography Interface," Technical Report, W3C Consortium, 2002.
- [7] Wei Xu, V. N. Venkatakrishnan, R. Sekar, I. V. Ramakrishnan, "A Framework for Building Privacy-Conscious Composite Web Services," 2005.
- [8] A. Tumer, A. Dogac, H. Toroslu, "A Semantic-based User Privacy Protection Framework for Web Services," Proceeding of WWW'03 Workshop on E-Services and the Semantic Web (ESSW03), Budapest, Hungary, May 2003.
- [9] A. Rezgui, M. Ouzzani, A. Bouguettaya and B. Medjahed. "Preserving Privacy in Web Services," Proceeding of 4th International ACM Workshop on Web Information and Data Management, Virginia, USA, PP. 56-62, November 2002.
- [10] The Platform for Privacy Preferences 1.0 Specification, World Wide Web Consortium Recommendation, April 2002, <http://www.w3.org/TR/P3P/>
- [11] Reagle, J., and Cranor, L. F. "The Platform for Privacy Preferences," Communication of the ACM, Vol. 42(2), PP. 48-55.
- [12] Liam Peyton and Max Nozin, "Tracking Privacy Compliance in B2B Networks," ICE'04 Sixth International Conference on Electronic Commerce.
- [13] <http://www.scottnichol.com/nusoapintro.htm>.