International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2015INPRESSCO®, All Rights Reserved Available at http://inpressco.com/category/ijcet

Review Article

A Review on Enhancing Privacy Preservation of Web Service through Negotiation Mechanism

Ankita A.Datir[†*] and Amit Sahu[‡]

[†]Computer Science And Engg (CSE), SGBAU Amravati University, India
[‡]Amravati University, India

Abstract

Web service composition is a web technology which is use for combining the information from multiple sources into single application. This technique provides a special type of composition application that aims at integrating data from multiple data provider depending on user request. DaaS depend on the specified useful data can be supplied according to the user demand. The main use of DaaS is eliminating redundancy and reduces associated expenditures. It modifies the data via single update point for multiple users. This paper proposes a formal privacy model in order to extend DaaS description with privacy capabilities. DaaS composition approach allowing to verify the compatibilities between privacy requirements and policies in DaaS composition.

Keywords: *Service composition, DaaS Service, Privacy, Negotiation, Service Oriented Architecture*

1. Introduction

Web services have recently emerged as a popular medium for data publishing and sharing the data on the web. According to the World Wide Web Consortium (W3C) definition, a web service is a software application identified but a URI, whose interface and binding are capable of begin defined. Web services are software components that communicate using pervasive, standards-based Web technologies including HTTP and XML-based messaging. Web services are designed to be accessed by other applications and vary in complexity from simple operations, such as checking a banking account balance online, to complex processes running CRM (customer relationship management) or enterprise resource planning (ERP) systems. Since they are based on open standards such as HTTP and XML-based protocols including SOAP and WSDL, Web services are hardware, programming language, and operating system independent. This means that applications written in different programming languages and running on different platforms can seamlessly exchange data over intranets or the Internet using Web services. In these, the application services that are the mechanisms for publishing, managing, searching, and retrieving contents are being accessed through the use of standard protocols and data formats like HTTP and HTML. Client applications like as web browser can understand these standards can interact with the application services to perform various tasks like ordering home appliances, sending gift, or reading newspaper etc. Web service is nothing but the communication between two electronic device over the internet. Most of the web services use the Extensible markup language (XML) for storing the data. Web services are the popular medium of sharing the data over the network. Web services are use for Business to Business interaction.

This step is optional but is beneficial when a company wants its Web services to be discovered by internal and/or external service consumers. Based on information in the UDDI registry, the Web services client developer uses instructions in the WSDL to construct SOAP messages for exchanging data with the service over HTTP. More about these core technologies is detailed below. Web Services are self-description, platform independent and use open standards so different parties can communicate and work with each other easily. These features cause industry increasingly pay attention to this technology. With increasing web services usage, more and more threats and vulnerabilities are discovered. Attackers identify web service vulnerabilities and use them to penetrate system. Attackers steal sensitive consumer's information and reduce his privacy. Web service composition is a web technology that combines information from more than one source into a single web application. This technique provides a special type of composition application that aims at integrating data from multiple data providers depending on the user's request. The automatic selection, composition, and interoperation of Web services to perform some task, given a high-level description of an objective. A web

*Corresponding author: **Ankita A.Datir** service is any piece of software that makes itself available over the internet and uses a standardized XML messaging system. XML is used to encode all communications to a web service. Modern enterprises across all spectra are moving towards a service-oriented architecture by putting their databases behind Web services, thereby providing a well-documented, platform independent and interoperable method of interacting with their data. A web service is a software function provided at a network address over the web or the cloud, it is a service that is "always on" as in the concept of utility computing. DaaS (Data-as-a-Service) Services where services correspond to calls over the data sources. It is a cousin of software as a service. DaaS have started to be popular medium for the data publishing and sharing on the web. Most of the enterprises across all spectra are moving towards service oriented architecture by wrapping their data source in DaaS services. It is use for Business to Business (B2B) interaction.

2. Background

A Web Service is a method, or set of methods, that can be invoked over the internet or other network. A Web Service and its clients exchange information using only standard non-proprietary protocols: SOAP and HTTP, for example. This means that Web Services are both platform and programming language neutral. A .NET or Java application can, for example, be a client of a Web Service coded in MVBasic. An MVBasic application can be a client of a Web Service coded using Java or .NET.

The following table lists the principal Web Service protocols along with their purposes and provides a brief description of each protocol.

Protocol	Purpose	Description
HTTP	Transport	Hypertext Transfer Protocol. Basic networking protocol used by the internet.
SOAP	Packaging	Simple Object Access Protocol. An XML-based protocol for encoding messages sent between a Web Service method and a client. Encodes the arguments passed to a Web Service method as well as any values returned by the method to the client.
WSDL	Description	Web Service Description Language. An XML-based protocol for describing a Web Service. A WSDL document provides the location of the Web service, the signatures of a Web Services' methods as well as other information about the data types involved in the Web Service. Clients use the WSDL to generate proxy classes for accessing the Web Service.
UDDI	Discovery	Universal, Description, Discovery, and Integration. An XML-based protocol for creating Web Service registries that applications can use to locate Web Service descriptions.

3. Literature Survey

This section presents related literature concerning Privacy Preservation Web Services

In 2014, Salah-Eddine and Michale Mrissa has proposed a paper “Privacy-Enhanced Web Service Composition”, they proposed a dynamic privacy model for Web Services. This model deal with the privacy at the data and operational level.This paper proposed a Negotiation approach to tackle the incompatibilities between privacy policies and the requirements. For the specific purpose privacy polices is provided for the data and operational level. Privacy policies are used only for the private data. According to the user demand the negotiation privacy policies is provided to the data. Privacy policies always reflect the usage of private data as a specifies or agreed upon by service provider.

In 2012, Rui André Oliveira, Nuno Laranjeiro, Marco Vieira proposed a paper, “Experimental Evaluation of Web Service Frameworks in the Presence of Security Attacks”, In this paper they studied the behavior of well-known web services frameworks in the presence of security attacks targeting the core web services specifications, i.e., those enabling basic message exchange functionalities. Results show that frameworks are quite resistant to attacks. However, they also indicate that even very popular and highly tested frameworks can be vulnerable to attacks, with potentially catastrophic consequences for the services being deployed.In this paper, they proposed an experimental approach to evaluate the security of well-known and widely used web service stacks, namely: Metro 2.1.1, Apache CXF 2.5.1, Apache Axis 2 version 1.6.1, and Apache Axis 1 version. The approach is based on a set of attacks that have been compiled from diverse security research studies, current security tools, and field experience, and that target core WS messaging features . The compiled attacks are used in a set of runtime tests performed to assess the behavior of the frameworks in presence of malicious requests. Frameworks are then classified with the use of an adaptation of the CRASH scale.

In 2012, Omid Banaei and Siavash Khorsandi, “A New Quantitative Model for Web Service Security”, In this paper they proposed a hierarchical structure for web service security and present a model that compute step-by-step security state of web service. They considered all of security aspects and using weighted averaging and AHP Theory for prioritizing security requirements. They used weighted averaging in all levels of our model to adapt with provider/consumer requirements.

In 2011, Chi Po Cheong, Chris Chatwin, Rupert Young presented a paper on , "A New Secure Token For Enhancing Web Service Security", This paper proposes a new secure token for improving the existing Web Service Security standards which provide message integrity and message confidentiality. Service Oriented Architecture (SOA) is widely adopted and most of them use Web Services implemented using a Simple Object Access Protocol (SOAP), an XML document or message exchanges between sender and receiver using HTTP protocol. Security is critical because the message is transferred around a public network, the Internet. Whilst current Web Service Security Standards protect the message; the location of the message sender is not authenticated, this can be provided using the proposed token.

This paper presents a brief introduction to XML and Web Services security standards and their relationship. A new secure token has been proposed and it can be used for the authentication of a remote client location. The syntax and processing rule is also described in the paper. An SOA-based system can save system resources and accept more SOAP requests by rejecting invalid requests, which come from unknown or fake domains by adopting the proposed token.

In 2011, Tristan Lavarack and Marijke Coetzee proposed a paper, "Web services security policy assertion trade-offs**"**, this paper focuses on modeling the decisions and compromises to be made by web services providers or consumers to be able to interact with each other securely. The security policy support system built to model this problem employs domain vocabularies, fuzzy techniques and domain-specific preferences.

The proposed research introduces the use of fuzzy techniques for trade-off analysis for web services security policies. The security policy support system supports administrators to consider all security aspects found in the environment and the security policies with their interrelated effect when policy trade-offs are made to accommodate consumers. Administrators specify an initial set of security preferences and security goals using fuzzy linguistic terms to make it easier to express themselves and understand the results of the analysis. The system supports an operational security level, to alert administrators of changes.

4. Technique Used In Web Service

Instance management refers to a set of techniques used to bind a set of messages to a service instance. It's necessary because applications widely differ in their needs for scalability, performance, throughput, transactions, and queued calls, and there simply isn't a one-size-fits-all solution to address these varied demands. Understanding instance management is essential to developing scalable and consistent service-oriented applications.

By and large, the service instance mode is strictly a service-side implementation detail that should not manifest itself on the client side. Following three techniques used to manage web service

A. Per Call

Per-call services are the Web Service default instantiation mode. In case of Per Call Instance mode, a new instance is created against each request coming from client and later disposed off when response is sent back from service. In per call clients create the objects they need when the client application starts and dispose of them when the client application shuts down. What impedes scalability with the client-server model is that the client applications can hold onto objects for long periods of time, while actually using the objects for only a fraction of that time. If you allocate an object for each client, you will tie up such crucial or limited resources for long periods of time and you will eventually run out of resources.

B. Per Session

Web service can maintain a private session between a client and a particular service instance. When the client creates a new proxy to a service configured as session-aware, the client gets a new dedicated service instance that is independent of all other instances of the same service. That instance will remain in service usually until the client no longer needs it. Each private session uniquely binds a proxy to a particular service instance. Note that the client session has one service instance per proxy. If the client creates another proxy to the same or a different endpoint, that second proxy will be associated with a new instance and session.

Because the service instance remains in memory throughout the session, it can maintain state in memory, and the programming model is very much like that of the classic client-server model. Consequently, it also suffers from the same scalability and transaction issues as the classic client-server model. A service configured for private sessions cannot typically support more than a few dozen (or perhaps up to a few hundred) outstanding clients due to the cost associated with each such dedicated service instance.

C. Shareable Service

Web Service does not allow you to pass object references across service boundaries. Objects are technology-specific entities, and sharing objects goes against the grain of service-oriented, technology-neutral interactions. However, sometimes one client may want to share the current state of its session with another client. The solution is a shareable service. A shareable service behaves much like a per-session service, with one important additional aspect: the instance has a unique ID, and when a client establishes a session with a shareable service, the client can pass a logical reference to that instance to another client. The second client will establish an independent session but will share the same instance. Also, each of these sessions may use different inactivity timeouts, and expire independently of any other session.

Conclusions

This paper proposed different types of binding mechanism and dynamic privacy model on web service. The model deals with privacy at the data and operation levels. This system also proposed a negotiation approach to tackle the incompatibilities between privacy policies and requirements. Although privacy cannot be carelessly negotiated as typical data, it is still possible to negotiate a part of privacy policy for specific purposes. In any case, privacy policies always reflect the usage of private data as specified or agreed upon by service providers.

References

Salah-Eddine Tbahriti, Chirine Ghedira, Brahim Medjahed, Michael Mrissa ,(APRIL-JUNE 2014), "Privacy-Enhanced Web Service Composition", *IEEE transactions on services computing*, Vol. 7, No. 2.

Rui André Oliveira, Nuno Laranjeiro, Marco Vieira,(2012), "Experimental Evaluation of Web Service Frameworks in the Presence of Security Attacks", *IEEE , Ninth International Conference on Services Computing.*

D.Younxiang and G.Yang,(2011),"Evaluating Vulnerabilities quantitatively based on the rank of web services confidentiality"*Journal of Next Generation Information Technology,*vol.2,no 1.

Omid Banaei and Siavash Khorsandi,(2012), "A New Quantitative Model for Web Service Security", *IEEE*,978-1-4673-2101-3.

Chi Po Cheong, Chris Chatwin, Rupert Young,(2011), "A New Secure Token For Enhancing Web Service Security", *IEEE*, 978-1-4244-8728-8/11.

Tristan Lavarack and Marijke Coetzee ,(2011), "Web services security policy assertion trade-offs", *Sixth International Conference on Availability, Reliability and Security.*

M. Bartel, J. Boyer, B. Fox, B. LaMacchia, E. Simon,(10 June 2008), "XML Signature Syntax and Processing (Second Edition), *W3C Recommendation.*

A. Nadalin, C. Kaler, R. Monzillo, P. Hallam-Baker,(1 February 2006), "Web Service Security: SOAP Message Security 1.1", *OASIA Standard Specification.*