Security Issues concerning Web Services

Kendrick Eargle

Midlands Technical College
Columbia, SC 29202
Email: kearg24@yahoo.com

Goal:
Evaluate the feasibility of web service security annotation to support dynamic web service compositions.

Abstract

In this paper we examined the support of current web service technologies and how they provide security requirements. It is important for web service security to concentrate on topics such as access control, authentication, reliability in data, and privacy. Security is so important because web services communicate on a program to program basis. We want to make sure that the development of security levels is secure for messaging, otherwise critical data can be transmitted in an inappropriate manner, for example credit card information. Finding out how to implement a software application with the requirements that meet a web service composition based on levels of security, makes the design intriguing. This research presents a model of security that protects web services, based on the importance of information retrieved or transferred.

1. Introduction

Web services have expanded to become more popular with application developers and the technology represents an important way for businesses to communicate with each other and with clients. Web services do not provide the user with a GUI (Graphic User Interface), but they share business logic, data and processes through a programmatic interface across a network [1]. How web services might work to improve productivity in the modern business world is by contributing to the software used to enhance its performance, making the daily responsibilities for humans available to perform other duties [2].

Since the arrival of web services, the software industry has changed significantly, and developing security for such highly secure applications will be challenging. It is important for businesses to trust that this technology is secure, reliable, and capable of working with distinct products in the same network [2]. The first consideration when developing security are the concerns, such as monitoring network traffic, exposure to software bugs, unauthorized access to resources, malicious attacks, etc [3]. These security concerns will play a pivotal role in the development stages, and depending on how significant the products or data to be processed are valued will also contribute on the level of security.
Since the web is organized globally with information contained on a system that enables humans to retrieve resources, security is very important for the retrieval of these resources. For example, restricted sites contain an authenticated login-password, SSL (secure socket layer) encryption of credit cards and other personal confidential information [6]. Security for web services is highly related to this type of access and since they communicate from program to program, making sure that the communication is secret is important as well. Keeping the communication secret is done through a process called cryptography. Cryptography attaches the identity to a message that the user can see, understand and trust [6]. Cryptography is the base source to keep any information the user may input to be confidential and kept out of harms way. My model is similar to this process because it detects what type of information is being retrieved or sent, and enforces the security based on those requirements.

The outline of this paper is as follows. In section 2, I describe in distinctive detail the background of various important web service technologies. Section 3 briefly describes examples of related work and different approaches concerning this topic of study, such as web service security annotation, web service compositions (BPEL). Section 4 explains an analysis of technology that web services support and future direction for web service annotation. Section 5 concludes the current research and expresses opinions on this topic.

2. Background

Related works based on the security of web services have proven that technologies to protect these services are becoming more difficult, due to the varying levels of security. Recent research resulted in the design of Service Orientated Architecture (SOA). His project was modeled to orchestrate services into composite services based on security requirements of individual services. Using military standards, he developed a lattice structure that described how levels of security are based on the classification of its service [4].

Some of the basic technologies used to describe and incorporate web services are Extensible Markup Language (XML), Simple Object Access Protocol (SOAP); web Services Description Language (WSDL) and Universal Description, Discovery, and Integration (UDDI) platform elements over an IP backbone. XML is used to label data, SOAP is used to relocate data, WSDL is used to give a description of available services and UDDI is used detecting what services are available [1].

2.1 **UDDI** and **WSDL**

UDDI (Universal Description, Discovery, and Integration) is the base for locating the web services. This is where WSDL is stored. It registers available services and in what way they are stored, how they are administered about service providers, service implementation, and service metadata [2]. Basically UDDI is a type of directory where information can be retrieved from various providers. WSDL is formatted similar to the XML language and it examines the abilities of web services as a group of communication endpoints of distributing messages [2].
2.2 WS-BPEL

When Multiple web services are composed together to form a more complex web service, the process is called WS-BPEL. The compositions of these services rely heavily on the syntactic level which will affect the structure of more than one web service composition [5]. WS-BPEL allows the export and import of the functionality by using web service interfaces exclusively [4]. WS-BPEL provides an organization for illustrating exchanges of information internally and externally, and it primarily deals with the function of the business process. It allows business to interact using web services and it applies a XML-base grammar for describing the logic to manage and guide web services to interact with the process [9].

2.3 XML and XML Schema

XML is an extensible markup language from HTML, and has been reformed to make implementation easier and more efficient. This language is a detachment from SGML (Standard Generalized Markup Language) and specifically designed for web documents. XML documents are made up of entities of parsed or unparsed data. Characters are made up of data that are parsed and it forms a markup, which makes up the logical structure of a document [8]. The structure of web services depends on how well it is documented. XML Schema makes it possible to document at a high level, creating a more efficient and easier way to compose web Services. XML Schema plays a vital part in the XML family, and as it relates to web Services, is the key advancement of enabling incorporation. It can also be known as instance documents, and XML technologies can be compared with object orientation which contains objects that are stored in classes, which are known as instances. Concluding that XML schemas are the classes and XML documents are the objects, and the documents are included the schemas making it a great asset for organization [11].

2.4 SOAP

As described earlier, SOAP messages are used to relocate data. Sending these messages between modules is similar to how we communicate with a service to retrieve data from a resource or transfer data [7]. SOAP messages are pivotal to web services because they encode the messages from a web service request using rash XML protocol and make sure the information is adequate before it is sent over a network.

Given the ubiquitous use of web services on the internet, security is tough to implement because of the variety of global data being enforced. My proposal somewhat introduces a new approach that examines the data and applies the appropriate security level to protect the information in a secure manner.

3. Related Work
3.1 **Web Service Industry**

Web services have made a major progress since their introduction. Due to the vast usage of web services the industry is growing at a rapid rate. The concept of using Remote Procedure Call (RPC) was not successful due to the fact that users had more boundaries where he/she could explore the web [12]. Developing an approach that would expunge more boundaries and expand the web to become global made the web service industry in web service like none other. Web services are primarily messaged based commuting from services to providers. The most important procedure was to provide a sensible way to make these messages better suited for providing better privacy in the industry. Using WSDL ensures that potential customers can access the service, without the understanding of how the actual service logic is executed [13], theoretically making the service better equipped and securely safe from outsiders.

3.2 **Web Service Security Annotation approach**

Due to the various approaches in web service security, many developers have elaborated on the security standards for web services and how the ontologies describe the characteristics of the security. This annotation approach uses the mark up language known as DARPA Agent Markup Language (DAML) and allows the annotation of web pages to illustrate it purpose. DAML is used to examine the capabilities of services and procedures on the web. The core of this approach expresses the security aspects of web services and its annotated capabilities can be utilized in situations where agents explore for web services with particular security requirements [10].

4. **Analysis of Technology for Web Service Annotation**

4.1 **My Research**

The global importance of securing critical data has increased concern for the security characteristics of web services. Accessing different services requires a more sufficient security approach. In this paper, analysis of a proposed model is presented explaining how security requirements can be implemented in such a way to detect what level is required.

4.1.1

There are 3 level of security: Top Secret (TS), Secret (S), and Public (P). When a user attempts to access information, one of these three levels is applied to the web service as one security level. The current issue is, “What level of security should be applied?”
4.1.2

My proposal suggests a type of packaging program that would be implemented with the requirements to detect and select the proper level of security. For example, if a user tries access information classification as public level security, which would allow anyone to view at anytime then the selected security level would be public. Accessing information on a public level security would have the basic standards and would not require any personal information from the user.

4.1.3

When a request for information falls in the level that applies to secret security, the approach for its access differs from the public requirements. In this case the requirements would ask the user to create a login-in username and password. The reason for asking for the username and password is to ensure the user’s privacy and to apply the appropriate security level. The secret level security would limit the user to access certain information based on the security standards.

4.1.4

The approach for top secret level of security has more confidential information; therefore will prompt for more personal data from the user. Such as the username, password, address, social security, etc. Asking the user for this information will ensure that if the user attempts to access data that is prohibited, especially on a top secret level then locating the user will be easier to track down.

4.1.5

To make the web service wrapper program more efficient; key information regarding user’s time and date of access would be maintained. This would also make choosing the appropriate security level simple, if a new user were to access the same level of security that was previously accessed. Then the new information would overwrite the previously accessed information instead of going through a new process. This method only applies to the public level security because secret and top secret requires for more information from the user and this method would allow anyone access.

5. Conclusion
In this paper you read about the background and various technologies used to support web services. The research discusses the security issues and how applying the appropriate security level is vital to the information retrieved or transferred. Using XML schema to document and compose web services makes up the structure. Depending on how well the schema is documented will affect the structure of the web service. You learned how the industry of web services has grown significantly over the last decade, especially the improvement of global communication. Communicating worldwide has made the access of information more vulnerable to be obtained in the wrong hands. The security related issues has been discussed recently and this proposal can contribute to help resolve concerns of web service security.