Protection against Denial of Service and Input Manipulation Vulnerabilities in Service Oriented Architecture

Alwyn Roshan Pais, Deepak D.J., and B.R. Chandavarkar

Department of Computer Science and Engineering,
National Institute of Technology,
Karnataka (NITK), Surathkal, India
{alwyn.pais,deepak3884}@gmail.com, sai_srajan@yahoo.co.in

Abstract. Organizations are increasingly adopting Service Oriented Architecture (SOA) to build their distributed applications. SOA is a computing paradigm, emphasizing dynamic service discovery composition and interoperability. Web services are a technology that can be used to implement SOA and are increasingly becoming the SOA implementation of choice. Because a Web service relies on some of the same underlying HTTP and Web-based architecture as common Web applications, it is susceptible to similar threats and vulnerabilities. There are many vulnerabilities in web services such as SQL injection, Denial of Service, etc. that cannot be detected by web service standards and conventional firewalls. In this paper, we present a detailed design of XML firewall that can be used to prevent different vulnerabilities by validating the input xml documents before being processed by the web services. Also the XML firewall does the function of authentication, authorization and session management. We designed a modular architecture for XML firewall where each module checks for a particular vulnerability. We have also developed methods to detect and prevent SQL injection and Denial of Service vulnerabilities.

Keywords: Service Oriented Architecture, XML firewall, Web services, Input manipulation, Denial of service (DOS), XDOS, SQL Injection , SOAP, Web Service Security.

1 Introduction

A service-oriented architecture is essentially a collection of services. These services communicate with each other. Services are well-defined units of functionality that are accessible over the network via standard protocols [14]. They are invoked by software, and are not accessed by a human user. In other words, services are more like a remote procedure calls. The system that implements a service is called a provider, while the system that uses the service is called a consumer. The central standards relevant to service implementation and deployment are XML, SOAP, WSDL, and UDDI and services that conform to these standards are called web services.

D.C. Wyld et al. (Eds.): CNSA 2011, CCIS 196, pp. 331–343, 2011.

A web service is actually a collection of individual service operations, each of which can be thought of as an individual procedure.

As more businesses deploy web services over the internet that dynamically interact with various applications and data sources, the issue of how to secure them from intruders and possible threats becomes more important. According to OSVDB and NVD Input manipulation, Information disclosure and Denial of service vulnerabilities account for more than 90% of the total vulnerabilities found as on February 2009 [1].

2 Related Work

Web service security is an important part of Service Oriented Architecture environment since web service is the preferred choice of implementation of SOA. There are many research works are being done on Web service security. The proposed XML firewall is based Role Based Access Control (RBAC) model [5]. RBAC model is used in many of the security solutions provided in the distributed computing environment.

Previous work on web service security based on XML firewall was done by Haiping Xu et al. [4] which were based on Coloured Petri Nets (CPN). They proposed a formal XML firewall security model which consists of two major components, namely the application model and the XML firewall model, which are designed compositionally using colored Petri nets. They developed a compositional CPN model for XML firewall protected service-oriented systems. But the work did not give any details of how to detect and prevent different vulnerabilities [2].

Similar work on XML firewall was a SOA state XML firewall which gave a design of state based firewall architecture that supports role based access control detection of XML based attacks. The state-based XML firewall was designed as a software module with four functional components, namely client interface, RBAC processor, SOAP filter, and admin interface, which coordinate to protect the web services deployed on a web server. The access policies and the detection rules are modularized so that they can be dynamically updated without recompiling and reinstalling the XML firewall. The work explains the design of XML firewall but there were no implementation details and results regarding the performance and testing [15].

Denial of service attack on web services has been researched by few researchers like Gruschka et al. in his paper "Preventing Web Services Dos attack by SOAP message validation" [8], has presented a method to validate each incoming soap request for XML and schema validation , which in turn increases overhead of system. Another work in same area is done by Srinivas Padmanabhuni et al. [11] where he proposes a Patricia trie based representation so that schema and request message can be validated in efficient manner.

The research on SQL injection in web services was done by Nuno Antunes and Marco Vieira [18].The goal was to study the effectiveness of the scanners and to try to identify common types of vulnerabilities in web services environments. The results showed that many of the services tested were deployed without proper security testing as a large number of vulnerabilities were observed. They compared some of the existing web vulnerability scanners. They use a representative workload to exercise the services and understand the expected behavior and the typical responses in the presence of valid inputs. A Classification of SQL Injection attacks and the