A Multiagent Solution to Adaptively Classify SOAP Message and Protect against DoS Attack

Cristian I. Pinzón, Juan F. De Paz, Javier Bajo, and Juan M. Corchado

Universidad de Salamanca, Plaza de la Merced s/n, 37008, Salamanca, Spain
{cristian_ivanp,fcofds,jbajope,corchado}@usal.es

Abstract. SOAP messages use XML code, which makes them vulnerable to denial of service (DoS) attacks and puts the availability of web services at risk. This article presents an adaptive solution for dealing with DoS attacks in web service environments. The solution proposes a distributed hierarchical multiagent architecture that implements a robust mechanism of classification based on an advanced CBR-BDI agent. The agent incorporates a case-based reasoning engine that integrate a Perceptron Multilayer neural network during the re-use phase to classify incoming SOAP messages and reject those that are considered malicious. A prototype of the architecture was developed and the results obtained are presented in this study.

Keywords: SOAP message, XML Security, multiagent systems, CBR, ANN.

1 Introduction

In order to obtain interoperability between web service platforms, communication between web servers is carried out via an exchange of messages. These messages, referred to as SOAP messages, are based on standard XML and are primarily exchanged using HTTP (Hyper Text Transfer Protocol) [1]. XML messages must be parsed in the server, which opens the possibility of an attack if the messages themselves are not well structured or if they include some type of malicious code. Resources available in the server (memory and CPU cycles) can be drastically reduced or exhausted while a malicious SOAP message is being parsed. This type of attack is known as a denial of service (DoS) attack and is perpetrated at the web service level because of the intrinsic relationship it has with the XML standard for coding SOAP messages.

A number of standards for guaranteeing the security of messages have been proposed to date, including WS-Security [2], WS-Policy [3], WS-Trust [4], WS-SecureConversation [5], etc. However, the proposed solutions focus exclusively on the aspects of message integrity and confidentiality, and user authentication and authorization [5].

This article presents a distributed hierarchical multiagent architecture for dealing with DoS attacks in web service environments. The architecture incorporates a CBR-BDI [7] agent with reasoning, learning and adaptation capabilities. The idea of a CBR mechanism is to exploit the experience gained from similar problems in the past and

P. Meseguer, L. Mandow, and R.M. Gasca (Eds.): CAEPIA 2009, LNAI 5988, pp. 181–190, 2010.

then adapt successful solutions to the current problem. The CBR engine initiates what is known as the CBR cycle, which is comprised of 4 phases. The classifier agent uses a Multilayer Perceptron neural network (MLP), which is incorporated into the re-use phase of the CBR cycle. By combining the CBR mechanism and the MLP, the system acquires learning capabilities and is able to adapt to changes in attack patterns for SOAP messages, thus facilitating the classification task when a SOAP message contains a DoS attack.

The rest of the paper is structured as follows: section 2 presents the problem that has prompted most of this research work. Section 3 focuses on the details of the multiagent architecture; section 4 explains in detail the classification model integrated within the classifier agent. Finally, section 5 describes how the classifier agent has been tested and presents the results obtained.

2 Web Service Security Problem Description

Attacks usually occur when the SOAP messages either come from a malicious user or are intercepted during the transmission by a malicious node that introduces different kinds of attacks.

The following list contains descriptions of some known types of attacks that can result in a DoS attack, as noted in [8] [9] [10].

- Oversize Payload: It reduces or eliminates the availability of a web service when a message with a large payload is parsed within the server.
- Coercive Parsing: An XML parser can analyze a complex format and lead to an attack because the memory and processing resources are being used up.
- Injection XML: The structure of a XML document is modified with a malicious code.
- SOAP header attack: Some SOAP message headers are overwritten while they are passing through different nodes before arriving at their destination.
- Replay Attack: Sent messages are completely valid, but they are sent en masse over short periods of time in order to overload the web service.

All web service security standards focus on strategies independent from DoS attacks [5]. In the following, we will revise those works that focus on denial of web service attacks and will compare to our approach as shown in Table 1.

A “XML Firewall” is proposed by [8]. Messages that are sent to a web service are intercepted and parsed to check the validity and the authenticity of the contents. If the contents of the messages do not conform to the policies that have been set, the messages will be dropped by the firewall. Gruschka and Luttenberger [6] propose an application level gateway system “Checkway”. They focus on a full grammatical validation of messages by Checkway before forwarding them to the server. Checkway generates an XML Schema from a web service description and validates all web service messages against this schema. An adaptive framework for the prevention and detection of intrusions was presented in [9]. Based on a hybrid focus that combines agents, data mining and diffused logic, it is supposed to filter attacks that are either already known or new. Agents that act as sensors are used to detect violations to the normal profile using the data mining technique such as clustering, association rules