A Security Proposal Based on a Real Time Agent to Protect Web Services Against DoS Attack

Cristian Pinzón, Angélica González, Manuel Rubio, and Javier Bajo

Abstract. This paper describes a novel proposal based on a real time agent to detect and block denial of service attacks within web services environments. The real time agent incorporates a classification mechanism based on a Case-Base Reasoning (CBR) model, where the different CBR phases are time bounded. In addition, the reuse phase of the CBR cycle incorporates a mixture of experts to choose a specific technique of classification depending on the feature of the attack and the available time to solve the classification.

Keywords: Multi-agent System, CBR, Web Service, SOAP Message, DoS attacks.

1 Introduction

New security issues as well as new ways of exploiting inherited old security threats can become a serious problem to applications based on web services. One of the threats that is becoming more common within web services environments and jeopardizes the availability factor is denial of service attack (DoS) [6] [5]. Since web services are a combination of a variety of technologies such as SOAP, HTTP, and XML, they are vulnerable to different type of attacks. For example, an attacker sends a malicious request (XML message) to the web service and the XML message forces the XML parser into an infinite recursion exhausting all

Cristian Pinzón
Universidad Tecnológica de Panamá, Av. Manuel Espinosa Batista, Panamá
e-mail: cristian_ivanp@usal.es

Angélica González · Manuel Rubio · Javier Bajo
Departamento Informática y Automática
Universidad de Salamanca
Plaza de la Merced s/n, 37008, Salamanca, Spain
e-mail:{angelica,mprc,jbajope}@usal.es

E. Corchado et al. (Eds.): SOCO 2010, AISC 73, pp. 1–8.

available computing resources. As a result, the attack prevents access the available services to the authorized users.

Response time is a critical aspect in the majority of internet security systems. This article presents a novel proposal to cope with DoS attacks, but unlike existing solutions [6], [5], [8], [10], [9], [2] our proposal takes into account the different mechanisms that can lead to a DoS attack. In addition, our proposal is based on a real time classifier agent that incorporates a mixture of experts to choose a specific technique of classification depending on the feature of the attack and the available time to solve the classification. The internal structure of the agent is based on the Case-Base Reasoning (CBR) model [3], with the main difference being that the different CBR phases are time bounded, thus enabling its use in real time.

The rest of the paper is structured as follows: section 2 presents the problem that has prompted most of this research work. Section 3 shows a general view of the temporal bounded CBR used as deliberative mechanism in the classifier agent. Section 4 explains in detail the classification model designed. Finally, the conclusions of our work are presented in section 5.

2 DoS Attacks Description

With XML and Web Services the risk of a DoS attack being carried out increases considerably. The most common message protocol for Web Services is SOAP, an XML based message format. Such a SOAP message is usually transported using the HTTP protocol. The DoS attacks at the web services level generally take advantage of the costly process that may be associated with certain types of requests.

Table 1 presents the types of DoS attack analyzed within this study.

Table 1 Types of attacks

Types of Attacks	Description
Recursive Payloads	A message written in XML can harbor as many elements as required, complicating the structure to the point of overloading the parser.
Oversize Payloads	It reduces or eliminates the availability of a web service while the CPU, memory or bandwidth are being tied up by a massive mailing with a large payload.
Buffer overflow	This attack targets the SOAP engine through the Web server. An attacker sends more input than the program can handle, which can cause the service to crash.
XML Injection	Any element that is maliciously added to the XML structure of the message can reach and even block the actual Web service application.
SQL Injection	An attacker inserts and executes malicious SQL statements into XML
XPath Injection	An attacker forms SQL-like queries on an XML document using XPath to extract an XML database.

It is important to understand that the focus of our proposal centers on the classification of web service requests through SOAP messages. Finally, there are several initiatives within this field: [6], [5], [8], [10], [9], [2]. However, the main disadvantage common to each of these approaches is their low capacity to adapt