Protecting Web Services against DoS Attacks: A Case-Based Reasoning Approach

Cristian Pinzón[1, 2], Juan F. De Paz[2], Carolina Zato[2], and Javier Pérez[2]

[1] Universidad Tecnológica de Panamá, Av. Manuel Espinosa Batista, Panama
[2] Departamento Informática y Automática, Universidad de Salamanca, Plaza de la Merced s/n, 37008, Salamanca, Spain
{cristian_ivanp,fcofds,carol_zato,jbajope}@usal.es

Abstract. The real-time detection is a key factor to detect and block DoS attacks within Web services. DoS attacks can be generated for different techniques that take advantage of points vulnerable within Web services. This paper describes a novel proposal based on a real time agent to classify user requests and detect and block malicious SOAP messages. The classification mechanism is based on a Case-Base Reasoning (CBR) model, where the different CBR phases are time bounded. Within the reuse phase of the CBR cycle is incorporated a mixture of experts to choose the most suitable technique of classification depending on the feature of the attack and the available time to solve the classification. A prototype of the architecture was developed and the results obtained are presented in this study.

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

1 Introduction

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. One of the threats that is becoming more common within web services environments and jeopardizes the availability factor is denial of service attack (DoS) [1-2]. Some security mechanism such as traditional layer 2-4 firewalls and even application level firewalls are no longer viewed as an effective way for providing a solution to this new threat.

The real-time detection is an important requirement for security systems, mainly when the threats are related with DoS attacks. With systems requiring a response to be given before a specific deadline, as determined by the system needs, it is essential that the execution times for each of the tasks carried out by the system are predictable and able to guarantee a correct execution within the time needed for the given response. This article presents a novel proposal to cope with DoS attacks, but unlike existing solutions [1-5] our proposal takes into account the different mechanisms that can lead to a DoS attack within Web services for example (Recursive Payloads, XML Injection, SQL Injection, etc). 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

M. Graña Romay et al. (Eds.): HAIS 2010, Part I, LNAI 6076, pp. 229–236, 2010.

(CBR) model [6], 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 and results of our work are presented in section 5.

2 Denial of Service Attacks Description

Recently the availability of web services has been threatened by a well known and studied type of attack known as denial of service (DoS). With XML 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.

A DoS attack mechanism can affect the availability of web services to a greater or lesser degree depending on the complexity of the type of attack used and the target component of the attack. 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: [1-5]. However, the main disadvantage common to each of these approaches is their low capacity to adapt themselves to the changes in the patterns, which reduces the effectiveness of these methods when slight variations in the behaviours of the known attacks occur or when new attacks appear. Moreover, most of the existing approaches are based on a centralized perspective. Because of this and the focus on performance aspects, centralized approaches can become a bottleneck when security is broken, causing a reduction of the overall performance of the application. In addition, none of these approaches considers the limitations or restrictions in the response time.