An Adaptive Multi-agent Solution to Detect DoS Attack in SOAP Messages

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

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

Abstract. A SOAP message can be affected by a DoS attack if the incoming message has been either created or modified maliciously. The specifications of existing security standards do not focus on this type of attack. This article presents a novel distributed and adaptive approach for dealing with DoS attacks in Web Service environments, which represents an alternative to the existing centralized solutions. The solution proposes a distributed hierarchical multi-agent architecture that implements a classification mechanism in two phases. The main benefits of the approach are the distributed capabilities of the multi-agent systems and the self-adaption ability to the changes that occur in the patterns of attack. A prototype of the architecture was developed and the results obtained are presented in this study.

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

1 Introduction

The Web services processing model requires the ability to secure SOAP messages and XML documents as they are forwarded along potentially long and complex chains of consumer, provider, and intermediary services. However all standards that have been proposed to date, such as WS-Security [1], WS-Policy [2], WS-Trust [3], WS-SecureConversation [4], etc. focus on the aspects of message integrity and confidentiality and user authentication and authorization [5].

Until now, denial-of-service (DoS) attacks have not been dealt with in Web Services environments. A DoS attack on Web Services takes advantage of the time involved in processing XML formatted SOAP messages. The DoS attack is successfully carried out when it manages to severely compromise legitimate user access to services and resources. 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 article presents a novel distributed multi-agent architecture for dealing with DoS attacks in Web Services environments. Additionally, the architecture has a four-tiered

Á. Herrero et al. (Eds.): Computational Intel. in Security for Info. Systems, AISC 63, pp. 77–84.
springerlink.com

hierarchical design that is better capable of task distribution and error recovery. The most important characteristic of the proposed solution is the two-phased mechanism that was designed to classify SOAP messages. The first phase applies the initial filter for detecting simple attacks without requiring an excessive amount of resources. The second phase involves a more complex process which ends up using a significantly higher amount of resources. Each of the phases incorporates a CBR-BDI [6] agent with reasoning, learning and adaptation capabilities. The CBR engine initiates what is known as the CBR cycle, which is comprised of 4 phases. The first agent uses a decision tree and the second a neural network, each of which is incorporated into the respective reuse phase of the CBR cycle. As a result, the system can learn and adapt to the attacks and the changes in the techniques used in the attacks.

The rest of the paper is structured as follows: section 2 presents the problem that has prompted most of this research. Section 3 focuses on the design of the proposed architecture. Finally, section 4 presents the results and conclusions obtained by the research.

2 DoS Attacks Description

One of the most frequent techniques of a DoS attack is to exhaust available resources (memory, CPU cycles, and bandwidth) on the host server. The probability of a DoS attack increases with applications providing Web Services because of their intrinsic use of the XML standard. In order to obtain interoperability between platforms, communication between web servers is carried out via an exchange of messages. These messages, referred to as SOAP messages, are based on XML standard and are primarily exchanged using HTTP (Hyper Text Transfer Protocol) [7]. The server uses a parser, such as DOM, Xerces, etc. to syntactically analyze all incoming XML formatted SOAP messages. When the server draws too much of its available resources to parse SOAP messages that are either poorly written or include a malicious code, it risks becoming completely blocked.

Attacks usually occur when the SOAP message either comes from a malicious user or is intercepted during its 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 the CPU, memory or bandwidth are being tied up by the processing of messages with an enormous payload.
- **Coercive Parsing:** Just like a message written with XML, an XML parser can analyze a complex format and lead to an attack when the memory and processing resources of the server are being used up.
- **Injection XML:** This is based on the ability to modify the structure of an XML document when an unfiltered user entry goes directly to the XML stream. The message is captured and modified during its transmission.