A Solution CBR Agent-Based to Classify SOAP Message within SOA Environments

Cristian Pinzón, Belén Pérez, Angélica González,
Ana de Luís y, and J.A. Román

University of Salamanca, Plaza de la Merced s/n, 37008, Salamanca, Spain
{cristian_ivanp,lancho,angelica,adeluis,zjarg}@usal.es

Abstract. This paper presents the core component of a solution based on agent technology specifically adapted for the classification of SOA messages. These messages can carry out attacks that target the applications providing Web Services. An advanced mechanism of classification designed in two phases incorporates a CBR-Agent type for classifying the incoming SOAP messages as legal or malicious. Its main feature involves the use of decision trees, fuzzy logic rules and neural networks for filtering attacks.

Keywords: SOAP message, XML security, multi-agent systems, case-based reasoning.

1 Introduction

The communication among services based on Service Oriented Architecture Web Services (SOA) is carried out by XML-based messages, called SOAP messages. This message exchange process is one of the key elements required in SOA environments for system integration [1]. The SOAP message payload often consists of sensitive information, which is sent through insecure channels such as HTTP connections. If a malicious user playing the role of a middleman intercepts a message between sender and recipient, it can result in a series of malicious tasks carried out over the captured message. A number of technologies and solutions have been proposed for addressing the secure exchange of SOAP message. Some WS standards such as WS-Security [2], WS-Policy [3], among others, continually strive to provide real security. Within academia some solutions in the research & development phase focusing on web service security in greater detail are [1], [4], [5]. However, both the WS-Security Standards and the given solutions still do not provide full security, leaving gaps that can be exploited by any malicious user.

This paper presents the core component of a strong solution based on a multi-agent architecture for tackling the security issue of the Web Service. This core is embedded in a CBR-BDI [6] deliberative agent based on the BDI (Belief, Desire, Intention) [7] model specifically adapted for preventing many attacks over web services. Our study applies a solution in two phases that include novel case-based reasoning (CBR) [8] classification mechanisms. The first phase incorporates decision tree and fuzzy logic rules [9] while the second phase incorporates neural networks capable of making short term predictions [10]. The idea of a CBR mechanism is to exploit the experience

E. Corchado et al. (Eds.): HAIS 2009, LNAI 5572, pp. 492–499, 2009.

gained from similar problems in the past and to adapt a successful solution to the current problem. The CBR-BDI agent explained in this work uses the CBR concept to gain autonomy and improve its problem-solving capabilities. The approach presented in this paper is entirely new and offers a different way to confront the security problem in SOA environments.

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 structure of the classifier agent which facilitates classification of SOAP message, and section 4 provides a detailed explanation of the classification model integrated within the classifier agent. Finally, section 5 presents the conclusions obtained by the research.

2 Web Service Security Problem Description

A web service is a software module designed to support interaction between heterogeneous groups within a network. 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 standard XML (eXtensible Markup Language) and are primarily exchanged using HTTP (Hyper Text Transfer Protocol) [11].

Security is one of the greatest concerns within web service implementations. 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 different types of attacks, compiled from those noted in [4], [5], [12].

- Oversize Payload: When it is executed, it reduces or eliminates the availability of a web service while the CPU, memory or bandwidth are being tied up by a massive message dispatch with a large payload.
- Coercive Parsing: Just like a message written with XML, an XML parser can analyze a complex format and lead to a denial of service attack because the memory and processing resources 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 or the message is captured and modified during its transmission.
- Parameter Tampering: A malicious user employs web service entries to manually or automatically (dictionaries attack) execute different types of tests and produce an unexpected response from the server.
- SOAP header attack: Some SOAP message headers are overwritten while they are passing through different nodes before arriving at their destination. It is possible to modify certain fields with malicious code.
- Replay Attack: Sent messages are completely valid, but they are sent en masse over a small time frame in order to overload the web service.

Standards such as WS-Security [2] and WS-Policy [3], among others, have set the standard for solutions to security breaches. One solution proposed by [1] takes information from the actual message structure and adds a new header named *SOAP Account* that contains information on the message structure. One solution based on the