AIDeM: Agent-Based Intrusion Detection Mechanism

Cristian Pinzón, Martí Navarro, and Javier Bajo

Abstract. The availability of services can be comprimised if a service request sent to the web services server hides some form of attack within its contents. This article presents AIDeM (An Agent-Based Intrusion Detection Mechanism), an adaptive solution for dealing with DoS attacks in Web service environments. The solution proposes a two phased mechanism in which each phase incorporates a special type of CBR-BDI agent that functions as a classifier. In the first phase, a case-based reasoning (CBR) engine utilizes a Naïves Bayes strategy to carry out an initial filter, and in the second phase, a CBR engine incorporates a neural network to complete the classification mechanism. AIDeM has been applied within the FUSION@ architecture to improve its current security mechanism. A prototype of the architecture was developed and applied to a case study. The results obtained are presented in this study.

Keywords: Availability, Web Service Attack, Multi-agent, case-based reasoning.

1 Introduction

Security is one of the primary concerns in service oriented architectures (SOA) and Web services [1]. Some protective measures such as Web Service Security (WSS) [2], WS-Policy [3], WS-Trust [4], etc. focus on authorization and authentication aspects to ensure confidentiality and integrity. However, they do not contemplate security problems that put the availability of Web services at risk. The

Cristian Pinzón
Universidad Tecnológica de Panamá, Av. Manuel Espinosa Batista, Panama
e-mail: cristian.pinzon@utp.ac.pa

Martí Navarro
Departamento de Sistemas Informáticos y Computación, Universidad Polítecnica de Valencia, Camino de Veras s/n, 46022, Valencia, España
e-mail: mnavarro@dsic.upv.es

Javier Bajo
Escuela Universitaria de Informática, Universidad Pontificia de Salamanca, Compañia , 5 37002, Salamanca, Spain
e-mail: jbajope@upsa.es

Y. Demazeau et al. (Eds.): Trends in PAAMS, AISC 71, pp. 347–354.
springerlink.com

emergence of new threats that can interrupt the correct functioning of services is closely related to some of the components contained in this technology, such as the XML standard used to encode messages, and the hypertext transfer protocol (HTTP) used to the communication. Different types of threats, similar to denial of service (DOS) attacks, can incapacitate a web service and block access to authorized users by sending malicious requests to the web server.

This study presents AIDeM, an advanced detection method that can confront mechanisms or techniques that produce denial of service attacks within Web environments. AIDeM is intended to improve the initial security level within the FUSION@ architecture [5]. FUSION@ proposes a new and easier method to develop distributed intelligent ubiquitous systems, where applications and services can communicate in a distributed way with intelligent agents, even from mobile devices, regardless of time and location restrictions. FUSION@ did already include a security component within its structure consisting of an agent specialized. However, the security method employed by this agent is limited in scope making available services vulnerable to attack. AIDeM is based on a group of agents specially designed to work together intelligently and adaptively to solve the problem of the reliability of SOAP messages sent in service requests. The core of AIDeM is a classification mechanism that incorporates a two-phase strategy to classify SOAP messages. The first phase applies an initial filter for detecting simple attacks without requiring an excessive amount of resources. The second phase involves a more complex process that ends up using a significantly higher amount of resources. Each of the phases incorporates an intelligent agent that integrates a CBR engine with advanced classification capabilities. The idea of a CBR mechanism is to exploit the experience gained from similar problems in the past and then adapt successful solutions to the current problem [6]. The first agent uses a Naïves Bayes classifier and the second a neural network, each of which is incorporated into the respective re-use 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. Additionally, a strategy of a two phased classification mechanism is to use its resources (CPU, cycle, memory) and improve response time.

The rest of the paper is structured as follows: section 2 presents a general description of the FUSION@ architecture and the limitations of the current mechanism of security. Section 3 focuses on the details of the AIDeM architecture and the mechanism of classification. Finally, section 4 describes how the classifier agent has been tested inside a multi-agent system and presents the results obtained.

2 FUSION@ Architecture and Current Mechanism of Security

FUSION@ [5] combines a services-oriented approach with intelligent agents to obtain an innovative architecture that facilitates ubiquitous computation and communication, and high levels of human-system-environment interaction. It also provides an advanced flexibility and customization to easily add, modify or remove applications or services on demand, regardless of the programming language. FUSION@ framework defines four basic blocks: a) Applications represent