

An Attack Detection Mechanism Based on a Distributed Hierarchical Multi-agent Architecture for

View metadata, citation and similar papers at core.ac.uk

brought to you by  CORE

provided by Repositorio Institucional de la Universidad Tecnológica de...

Cristian Pinzón¹, Yanira de Paz², Rosa Cano³, and Manuel P. Rubio⁴

¹ Universidad Tecnológica de Panamá, Av. Manuel Espinosa Batista, Panama
cristian.pinzon@utp.ac.pa

² Universidad Europea de Madrid, Tajo s/n 28670, Villaviciosa de Odón, Spain
yanirarosario.depaz@uem.es

³ Instituto Tecnológico de Colima, Av. Tecnológico s/n, 28976, Mexico
rdegca@gmail.com

⁴ Escuela Politécnica Superior de Zamora, Av. Cardenal Cisneros 34, 49022, Zamora, Spain
mprc@usal.es

Abstract. This paper presents an innovative approach to detect and classify SQL injection attacks. The existing approaches are centralized while this proposal is based on a distributed hierarchical architecture to provide a robust and dynamic strategy. The strategy for the classification and detection of SQL injection attacks uses a combination based on detection by anomalies and misuses. The detection by anomaly uses a case-based reasoning mechanism incorporating a mixture of neural networks. The approach has been tested and the results are presented in this paper.

Keywords: SQL injection, Security database, IDS, Multi-agent, case-based reasoning.

1 Introduction

A potential security problem on the database is a SQL injection attack. This attack seriously affects the database and it takes place when an original query is modified and is executed on the database by a hacker. The SQL injection attack has been addressed by the majority of the proposal from a centralized perspective [1] [2]. The main drawback of these approaches is that they solve the SQL injection attacks partially. Other solutions more sophisticated apply intrusion detection techniques [3] [4], but they have as drawback their large rate of cases poorly classified.

The proposal presented in this work tackles the SQL injection attack problem through a distributed hierarchical multi-agent architecture. Within the architecture are implemented strategies based on misuse and anomaly detection [5]. The key component of the architecture is a type of BDI (Belief, Desire and Intention) deliberative agent [6] which incorporates a based-case reasoning (CBR) mechanism [7]. The idea of a CBR mechanism is to exploit the experience gained from similar problems in the past and to adapt then successful solution to the current problem. This CBR-BDI type of agent [8] has been specially adapted to resolve the SQL injection attack problem. This agents use the CBR concept to gain autonomy and improve their problem-solving

capabilities. In addition, it integrates a novel strategy of classification that lies in a mixture of neural networks which allows carrying out short term attack predictions. This work presents an entirely new approach in order to face the problem of SQL injection attack and describing an architecture that is unique in its conception.

The rest of the paper is structured as follows: section 2 presents the problem that has prompted most of this research work. Section 3 focuses on the details of the multi-agent architecture, section 4 explains in detail the classification model integrated within the classifier agent. Finally, section 5 describes how the classifier agent has been tested inside a multi-agent system and presents the results obtained.

2 SQL Injection Attacks

A SQL injection attack takes place when a hacker changes the semantic or syntactic logic of a SQL text string by inserting SQL keywords or special symbols within the original SQL command that will be executed at the database layer of an application [1] [9]. The results of this attack can produce unauthorized handling of data, retrieval of confidential information, and in the worst possible case, taking over control of application server. The main problem for the detecting of SQL injection attack is the large number of variants. The detection of some SQL injection results trivial whereas that the detection of other result extremely complex due to large number of possible strategies.

Nowadays, this type of attack has been handled from distinct perspectives. The string analysis [10] has been the support of many others approaches such as [1] and [11], which carried out an analysis more complete applying a treatment dynamic and hybrid over the SQL string. In other cases, artificial intelligence techniques have been applied to face the SQL injection attack, such as [12] with WAVES (Web Application Vulnerability and Error Scanner). This proposal uses a black-box technique which includes a machine learning approach. Valeur [3] presented an IDS approach which uses a machine learning technique based on a dataset of legal transactions. These are used during the training phase prior to monitoring and classifying malicious accesses. Rietta [4] proposed an IDS at the application layer using an anomaly detection model. Finally, Skaruz [13] proposed the use of a recurrent neural network (RNN). The detection problem becomes a time serial prediction problem. Usually, many approaches present a large number of false positive and false negative. The proposals based on intrusion detection depend on database, which requires a continue updating in order to detect new attacks.

Our approach takes advantage of the multi-agent system to reanalyze the problem in a distributed mode. Moreover, intrusion detection technique based on misuse and anomaly has been incorporated at strategic level into the architecture. The detection by anomaly is built by means of a case-based reasoning (CBR) mechanism [7], whose characteristics do it especially suitable to tackle classification problems and this is reinforced with the predictive capacity of a mixture of neural network [14]. The capture of SQL queries is carried out through of distributed agents and the detection can be executed in a distributed mode. Moreover, the architecture presents a high scalability, flexibility and learning capacity that allows it a greater adaptation for distributed environments and new strategic of attacks.