Unsupervised Visualization of SQL Attacks by Means of the SCMAS Architecture

Álvaro Herrero, Cristian I. Pinzón, Emilio Corchado, and Javier Bajo

Abstract. This paper presents an improvement of the SCMAS architecture aimed at securing SQL-run databases. The main goal of such architecture is the detection and prevention of SQL injection attacks. The improvement consists in the incorporation of unsupervised projection models for the visual inspection of SQL traffic. Through the obtained projections, SQL injection queries can be identified and subsequent actions can be taken. The proposed approach has been tested on a real dataset, and the obtained results are shown.

Keywords: Multiagent System for Security, Neural Projection Models, Unsupervised Learning, Database Security, SQL Injection Attacks.

1 Introduction

Over the last years, one of the most serious security threats to databases has been the SQL injection attack [1]. In spite of being a well-known type of attack, the SQL injection remains at the top of the published threat list [2]. The solutions proposed so far seem insufficient to block this type of attack because the vast majority of them are based on centralized mechanisms [3], [4] with little capacity to work in distributed and dynamic environments. Furthermore, the detection and classification mechanisms proposed by these solutions lack the learning and adaptation capabilities for dealing with attacks and variations of the attacks that may appear in the future.

Álvaro Herrero
Civil Engineering Department, University of Burgos
C/ Francisco de Vitoria s/n, 09006 Burgos, Spain
e-mail: ahcosio@ubu.es

Cristian I. Pinzón · Emilio Corchado · Javier Bajo
Departamento de Informática y Automática, Universidad de Salamanca,
Plaza de la Merced s/n 37008, Salamanca, Spain
e-mail : {cristian_ivanp,jbajope}@usal.es, escorchado@ubu.es

Y. Demazeau et al. (Eds.): Trends in PAAMS, AISC 71, pp. 713–720.
springerlink.com

This work presents a novel multiagent solution for anomaly visualization. The proposed multiagent system (MAS) is composed of agents with specialized abilities to detect and predict SQL injection attacks [5]. Most of the agents are focused on data monitoring and analysis. However, it is necessary to incorporate a new agent type with projection ability for anomaly visualization. This agent incorporates different projection models for data visualization, with the aim of notably improving the function of the MAS. As stated in [6], scant attention has been given to visualization in the security field, although visual presentations help operators and security managers to interpret large quantities of data. Several attempts have been made to apply connectionist models to the field of security, mainly based on a classificatory standpoint. A complementary approach is followed in this work, in which the main goal is to provide a data projection to visually identify SQL injection attacks. This idea has been previously applied in the field of Network Intrusion Detection [7].

The rest of the paper is structured as follows: Section 2 introduces the MAS architecture. Section 3 describes the unsupervised projection models. Section 4 shows the experimental results and, finally, Section 5 presents the obtained conclusions and the future work.

2 A Multiagent Solution for SQL Anomaly Visualization

The Structure Query Language (SQL) constitutes the backbone of many Database Management Systems (DBMSs), especially relational databases. It carries out information handling and database management, but it also facilitates building a type of attack that can be extremely lethal. SQL injection attacks are a potential threat at the application layer of the TCP/IP protocol stack. Although this type of attack has been the subject of many studies; it continues to be one of the most frequent attacks over the Internet. SQL injection occurs when the intended effect of the SQL sentence is changed by inserting SQL keywords or special symbols [1].

To deal with such attacks, the SCMAS architecture [5] has been upgraded by including a new type of agent named “Visualizer”, which provides the capacity of visualization. Its main function is to complement the classification of SQL attacks through visualization facilities. As a result, this new agent contributes to improving the classification performance of SCMAS. The SCMAS architecture proposes a novel strategy to block SQL injection attacks through a distributed approach based on the capacities of the SQLCBR agents, which are a particular type of CBR-BDI agents [8]. The architecture has been divided into four levels so that the specific tasks are assigned according to the degree of complexity. The different types of agents located at the different levels of the SCMAS architecture can be described as:

- Sensor: captures datagrams, orders TCP fragments to extract the request’s SQL string and executes a syntactic analysis of the request’s SQL string.