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.

- FingerPrint: performs a pattern matching of known attacks.
- DBPattern: updates and adds new patterns to the pattern database.
- Anomaly: this core component of the architecture carries out a classification of SQL strings through detection anomalies. It integrates a case based reasoning (CBR) mechanism.
- Manager: is responsible for the decision-making, evaluation and coordination of the overall operation of the architecture.
- Forecaster: predicts attacks by considering user behavior.
- LogUser: updates the profile of application users.
- DB: is responsible for executing queries to the database once the requests are classified as legal, and getting the results.
- Interface: facilitates the interaction between a human expert in charge of security and the SCMAS architecture. It can be run on mobile devices.
- Visualizer: this is the new type of agent proposed in this work for upgrading the SCMAS architecture. It applies different projection models for visualizing the SQL-related data, whose features are described in section 4.1. As a consequence of that, the SQL injection attacks can be visually identified.

Fig. 1 depicts the upgraded SCMAS architecture, incorporating the Visualizer agent and showing the different layers and their respective agents.

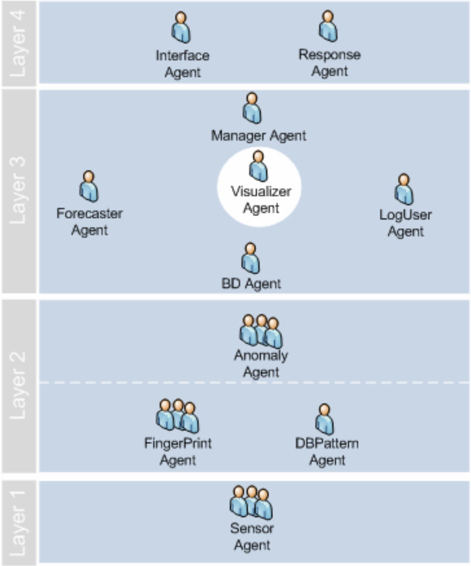


Fig. 1 Upgraded SCMAS architecture

3 Unsupervised Projection Models

Projection models are used as tools to identify and remove correlations between problem variables, which enable us to carry out dimensionality reduction, visualization or exploratory data analysis. In this study, some unsupervised statistical and neural projection models, namely Principal Component Analysis (PCA) [9], Curvilinear Component Analysis (CCA) [10], and Cooperative Maximum Likelihood Hebbian Learning (CMLHL) [11] have been applied, comparing their results.

PCA [9] is a standard statistical technique for compressing multidimensional data; it can be shown to give the best linear compression of the data in terms of least mean square error. PCA describes the variation in a set of multivariate data in terms of a set of uncorrelated variables each of which is a linear combination of the original variables. Its goal is to derive new variables, in decreasing order of importance, which are linear combinations of the original variables and are uncorrelated with each other.

CCA [10] is a nonlinear dimensionality reduction method. It was developed as an improvement on the Self Organizing Map (SOM) [12], trying to circumvent the limitations inherent in some linear models such as PCA. CCA is performed by a self-organised neural network calculating a vector quantization of the submanifold in the data set (input space) and a nonlinear projection of these quantising vectors toward an output space. As regards its goal, the projection part of CCA is similar to other nonlinear mapping methods, as it minimizes a cost function based on interpoint distances in both input and output spaces. Quantization and nonlinear mapping are separately performed: firstly, the input vectors are forced to become prototypes of the distribution using a vector quantization method, and then, a nonlinear mapping of the input vectors is built.

CMLHL [11] extends the MLHL model [13] that is a neural implementation of Exploratory Projection Pursuit (EPP) [14]. The statistical method of EPP linearly projects a data set onto a set of basis vectors which best reveal the interesting structure in data. CMLHL extends the MLHL model by adding lateral connections [11], which have been derived from the Rectified Gaussian Distribution [15]. Then, CMLHL finds the independent factors of a data set capturing some type of global ordering in the data.

Considering an N-dimensional input vector (x), and an M-dimensional output vector (y), with W_{ij} being the weight (linking input j to output i), then CMLHL can be expressed as:

1. Feed-forward step: $y_i = \sum_{j=1}^{\mathbf{N}} W_{ij} x_j, \forall i$ (1)

2. Lateral activation passing: $y_i(t+1) = \left[y_i(t) + \tau(b - Ay)\right]^{+}$ (2)

3. Feedback step: $e_j = x_j - \sum_{i=1}^{M} W_{ij} y_i, \forall j$ (3)

4. Weight change: $\Delta W_{ij} = \eta . y_i . sign(e_j) | e_j |^{p-1}$ (4)

Where: η is the learning rate, τ is the "strength" of the lateral connections, b the bias parameter, p a parameter related to the energy function [11], [13] and A is a symmetric matrix used to modify the response to the data [11]. The effect of this matrix is based on the relation between the distances separating the output neurons.

4 Experimental Results

To check the proposed Visualizer agents, several unsupervised projection models (introduced in section 2) have been applied to a real dataset containing samples of the target attacks.

In the projections shown in this section, normal queries are depicted as circles ('O'), while anomalous ones are depicted as crosses ('+'). This "class" information is used only for visualizations purposes. The projection models are not provided with such information while being trained as they are based on unsupervised learning.

4.1 Dataset

A web application with access to a database was developed to check the proposed approach. The web application manages a virtual store where different interfaces are available to carry out queries on the database. MySQL 5.0 was selected as the DBMS to support the web application. Once the database had been created, legal queries were sent from the designed user interfaces. These requests were filtered to avoid redundancy and only legal SQL queries were gathered to generate the dataset. However, in the case of malicious queries, the dispatch of the queries was automated using the tool SQLMap 0.5 [16]. This tool is able to fingerprint an extensive DBMS back-end, retrieve remote DBMS databases, usernames, tables, and columns, enumerate entire DBMS, read system files, and much more taking advantage of web application programming security flaws that lead to SQL injection vulnerabilities. Although the SQLMap 0.5 tool generates a wide variety of malicious queries by using different strategies of attack, these queries were also filtered to remove any similar SQL string previously stored.

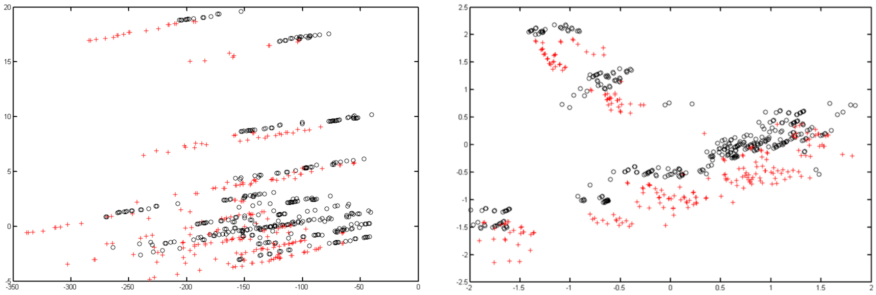
The dataset was formed by a set of 1,000 entries for legal and malicious queries. Finally, for the classification process and application of the projection models, the SQL strings were syntactically analyzed, storing in the dataset the fields described in Table 1.

Table 1. Dataset fields obtained from the syntactic analysis of SQL queries

Field	Description	Type (*Values)*
Affected_table	Number of *tables* affected by the query	Int (*n tables*)
Affected_field	Number of *fields* affected by the query	Int (*n fields*)
Command_type	Type of declared *command* in the query	Int (*0-3*)
Word_GroupBy	Number of repetitions of *Group By* clause	Int (*n clause*)
Word_Having	Number of repetitions of *Having* clause	Int (*n clause*)
Word_OrderBy	Number of repetitions of *Order By* clause	Int (*n clause*)
Numer_And	Number of repetitions of the *And* Operator	Int (*n ops*)
Numer_Or	Number of repetitions of the *Or* Operator	Int (*n ops*)
Number_literals	Number of *Literal* in the SQL string	Int (*n literals*)
Number_LOL	Number of declared Expressions *Literal-Operator-Literal* in the SQL String	Int (*n exprs*)
Length_SQL_String	Length of the SQL String	Int (*n chars*)

4.2 Experiments

The visualization capability of the Analyzer agent was tested by applying its projection models (PCA, CCA and CMLHL) to the aforementioned dataset. Fig. 2 shows the PCA and CMLHL projections of this dataset.



a) PCA projection.

b) CMLHL projection.

Fig. 2 Projections of the analysed dataset

The PCA projection (Fig. 2.a) is able to depict some structure of the analyzed dataset. Although these two first principal components amount to 99.7% of data variance, the depicted structure is not related with the normal/anomalous separation of data. That is, normal queries (circles) and anomalous queries (crosses) are mixed up in most of the groups that can be identified in Fig. 2.a.

Fig. 2.b shows the CMLHL projection of the analyzed dataset. Several clusters can be identified in this figure, most of them having a kind of internal organization differentiating normal queries from anomalous ones.

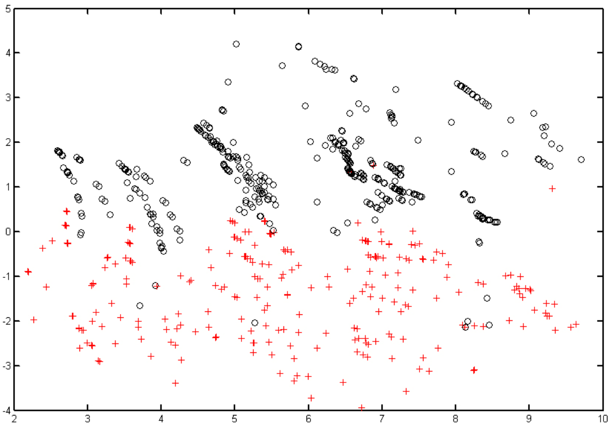


Fig. 3 CCA projection of the analysed dataset

Finally, CCA was applied to the dataset, as can be seen in Fig. 3. This projection model is able to depict the data in a way that most normal queries can be grouped, excluding the anomalous ones. Some normal and anomalous queries are overlapped, what would be considered as false positives/negatives.

From this experimental setup, we can conclude that CCA provides the best projection of the dataset under analysis, outperforming PCA and CMLHL. The CCA projection (Fig. 3) allows the visual identification of anomalous queries, as most of them can be distinguished from normal traffic.

5 Conclusions and Future Work

This paper presents a novel solution based on a new hierarchical MAS for visualizing SQL traffic. It allows the detection of SQL injection attacks by differentiating them from normal SQL queries. This solution combines the advantages of MASs, such as autonomy and distributed problem solving, with the visualization, learning and adaptation capabilities of unsupervised neural projection models. The proposed approach solves one of the lacks of the SCMAS architecture: the visualization of the data in an effective and intuitive way. Further work will focus on the combination of the new visualization abilities with the classification process

Acknowledgments. This research has been partially supported by the Spanish Ministry of Science project TIN2006-14630-C03-03, project of the Junta of Castilla and León BU006A08; Business intelligent for production within the framework of the technological Institute of Castilla y León and investment and services agency (ADE); project of the Spanish Ministry of Education and Innovation CIT-020000-2008-2. The authors would also like to thank the vehicle interior manufacturer, Grupo Antolin Ingenieria S.A., within the framework of the project MAGNO2008 - 1028.- CENIT Project funded by the Spanish Ministry.

References

1. Halfond, W.G.J., Viegas, J., Orso, A.: A Classification of SQL-Injection Attacks and Countermeasures. In: Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA (2006)
2. Breach Security Inc. The Web Hacking-Incidents Database (2008)
3. Halfond, W.G.J., Orso, A.: AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks. In: Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering (ASE 2005). ACM, New York (2005)
4. Kosuga, Y., Kono, K., Hanaoka, M., Hishiyama, M., Takahama, Y.: Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection. In: 23rd Annual Computer Security Applications Conference. IEEE Computer Society, Los Alamitos (2007)
5. Bajo, J., Corchado, J.M., Pinzón, C., Paz, Y.D., Pérez-Lancho, B.: SCMAS: A Distributed Hierarchical Multi-Agent Architecture for Blocking Attacks to Databases. International Journal of Innovative Computing, Information and Control (2008)
6. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., Stoner, E.: State of the Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99-TR-028. Carnegie Mellon University - Software Engineering Institute (2000)
7. Herrero, Á., Corchado, E., Gastaldo, P., Zunino, R.: Neural Projection Techniques for the Visual Inspection of Network Traffic. Neurocomputing 72(16-18), 3649–3658 (2009)
8. Corchado, J.M., Laza, R.: Constructing deliberative agents with case-based reasoning technology. International Journal of Intelligent Systems 18, 1227–1241 (2003)
9. Pearson, K.: On Lines and Planes of Closest Fit to Systems of Points in Space. Philosophical Magazine 2(6), 559–572 (1901)
10. Demartines, P., Herault, J.: Curvilinear Component Analysis: A Self-Organizing Neural Network for Nonlinear Mapping of Data Sets. IEEE Transactions on Neural Networks 8(1), 148–154 (1997)
11. Corchado, E., Fyfe, C.: Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors. International Journal of Pattern Recognition and Artificial Intelligence 17(8), 1447–1466 (2003)
12. Kohonen, T.: The Self-Organizing Map. IEEE 78(9), 1464–1480 (1990)
13. Corchado, E., MacDonald, D., Fyfe, C.: Maximum and Minimum Likelihood Hebbian Learning for Exploratory Projection Pursuit. Data Mining and Knowledge Discovery 8(3), 203–225 (2004)
14. Friedman, J.H., Tukey, J.W.: A Projection Pursuit Algorithm for Exploratory Data-Analysis. IEEE Transactions on Computers 23(9), 881–890 (1974)
15. Seung, H.S., Socci, N.D., Lee, D.: The Rectified Gaussian Distribution. Advances in Neural Information Processing Systems 10, 350–356 (1998)
16. Damele, B.: SQLMAP0.5 – Automated SQL Injection Tool (2007)