Automated detection system of insider attacks using fuzzy logic

Dodonov M.V., Dodonova N.L.

Samara State Aerospace University

Abstract. In this paper we design an insider threat monitoring system in the corporate information system. In the proposed system, fuzzy logic and the information about the current users' activity are used for effectively identifying the insider attacks.

Keywords: fuzzy logic, insider attacks, detection system.

Citation: Dodonov M.V., Dodonova N.L. Automated detection system of insider attacks using fuzzy logic. Proceedings of Information Technology and Nanotechnology (ITNT-2015), CEUR Workshop Proceedings, 2015; 1490: 376-380. DOI: 10.18287/1613-0073-2015-1490-376-380

In the modern corporate information systems (CIS) there is a huge amount of data, some part of which is classified as confidential. The confidential data play an important role in running of a successful commercial activity of a company. The theft of such information could lead to huge losses or bankruptcy of the company. From the standpoint of the data security, for the CIS there are two basic kinds of threats: the external threats and the internal ones. Now there is a sufficient number of decisions to protect the CIS from the external threats, whereas the techniques and methods for the CIS protection against the internal attacks are not yet sufficiently developed.

The systematic illegal activities of the CIS's own employees, who are called by the insiders, are now becoming the most common methods of the identity theft. By an insider we mean an employee who due to their official position has access to confidential information and use it in their own interests, perhaps going against the interests of the company.

Several types of potential insiders can be distinguished depending on the capabilities of the employee's access to an confidential information: top-rank authorities, privileged users, network engineers, maintenance staff of the CIS; employees who have access to the workstations (AWP) of the CIS, etc. This paper deals with one of the approaches for the protection of confidential information from the insiders in the CIS.

At present time, companies use various formal, technical and non-formal methods of information protection. In the paper we are focusing on the using of formal methods, and, more precisely, we will consider the possibilities of the software tools to detect the insider attacks. Usually companies bring out random monitoring of users with help of remote desktop, URL filtering and systems traffic counting. But one should remember that there is a probability that a responsible person may be in a collusion with a traced person and implement data theft. Therefore, an effective protection against an insider must be higher than the privileged users and the network engineers.

Along with trust to employees, a monitoring of the suspicious and the dangerous activities that can sometimes occur at user's workstations should not be neglected. For example, following issues have been increased greatly: the internal network traffic, the number of requests to the corporate database, the amount of printer toner or paper. These and many other events should be recorded and resolved, because behind them an attack or preparing for an attack on sensitive data can be hidden.

There are many scenarios that resolve the problem of information leakage (files, facts, databases, hard copies, etc.). The entry-level products allow us to track the leak channels, collect statistics of employees' requests to the objects of the confidential information, and close the ports and writer-reader systems. Higher-end solutions are based on applying broad range solutions that include, along with the above, network traffic analysis, monitoring of user operations with confidential information, etc.

A special feature of these complexes is the ability to lock access to the CIS device as well as the possibility of logging the users' activity with the help of monitoring agents. The main shortage of these systems is that they do not answer the question how to search for an insider. Moreover, these systems demand support and maintenance of highly qualified specialists, which cannot be afforded by a small-scale company. During the work of tracking programs large amount of data are being collected about user activity in the CIS. These data, together with additional information about employees, can be used for online monitoring of insider's attacks. At present time security specialist had to track individually accumulated data of used documents by employees and classification levels.

In this paper we propose appliance of an developed automated system that performs the following functions for the detection of the insider attacks:

- an gathering information from monitoring agents and stores it in a centralized database;
- an maintaining a database of user activity and additional information about them;
- an automatic calculation of the possible insider attacks using rules of fuzzy inference;
- an ability to add and edit linguistic variables;
- an ability to change the rules in the knowledge base;
- an ability to view the list of potential insiders among employees.

In the proposed system, a fuzzy logic deduction is use as the method of evaluation of an insider activity. It should be noted that the fuzzy logic is currently widely used for solving of various problems. Let us assume that there is an opportunity to gather an information about an employee that characterizes its activity related to the access to a confidential information. By the values of these characteristics it is possible to draw conclusions about the safety of employee's activities. Such conclusions may be based on different mathematical models.

The input data for the system is the information from the logs of the monitoring program agents performing control over usage of peripheral devices and other user activity. The output result data will be a list of employees indicating implement level of actions to insiders ones. The General scheme of the system can be seen in figure 1.

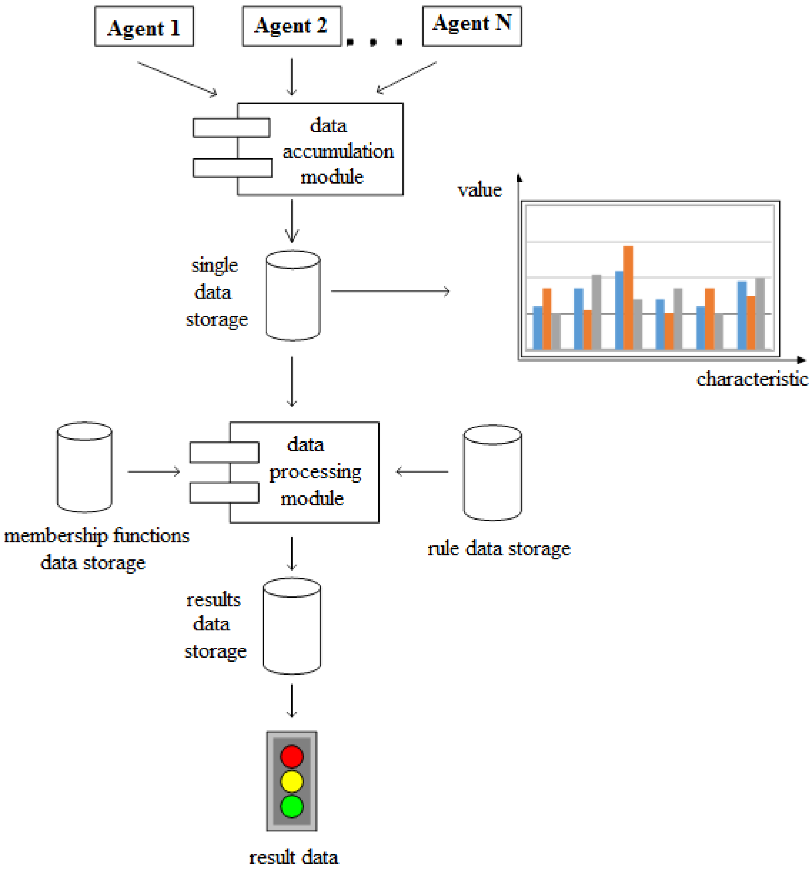

Fig. 1. – General scheme of the system

All information about employees’ activities flows into one databank through the accumulation module data. Following information is being collected into this data-bank with specific time interval (year, quarter, month, day, hour, etc.). In other words, data collection module receives information from monitoring program agents and distributes by employees activity characteristics (working hours, number of sent data, etc.). Whereas the units of measurement will be also incommensurable, so usage of fuzzy logical inference allows to obtain the desired result.

A single data storage was created to keep an information about the current activity of a company's employees (figure 2). The entity "Parameter_Value" keeps the relevant data collected by the software agents during the certain period of time. The data accumulation module processes the received information and keeps it in convenient form for further processing.

The data processing module based on the fuzzy inference with help the given by experts the membership functions and the rule base draws the conclusions on the activity of each employee and writes the results into the data storage.

Let us consider algorithm of data processing module in more detail. Let *X* will be some employee of the organization, which can be characterized by a set of characteristics (*V_1*, *V_2*, ... *V_n*). These characteristics take into account the work position of the employee, term of employment, his credentials, access and activity with confidential information, etc.

The assessment of individual activity from the viewpoint of the damage to the corporate security, can be described in terms of a natural language: "safe" and "likely safe" and "possibly dangerous", etc. Thus, the activity of the employee is set by the values of linguistic variables stored in the entity "Parameter".

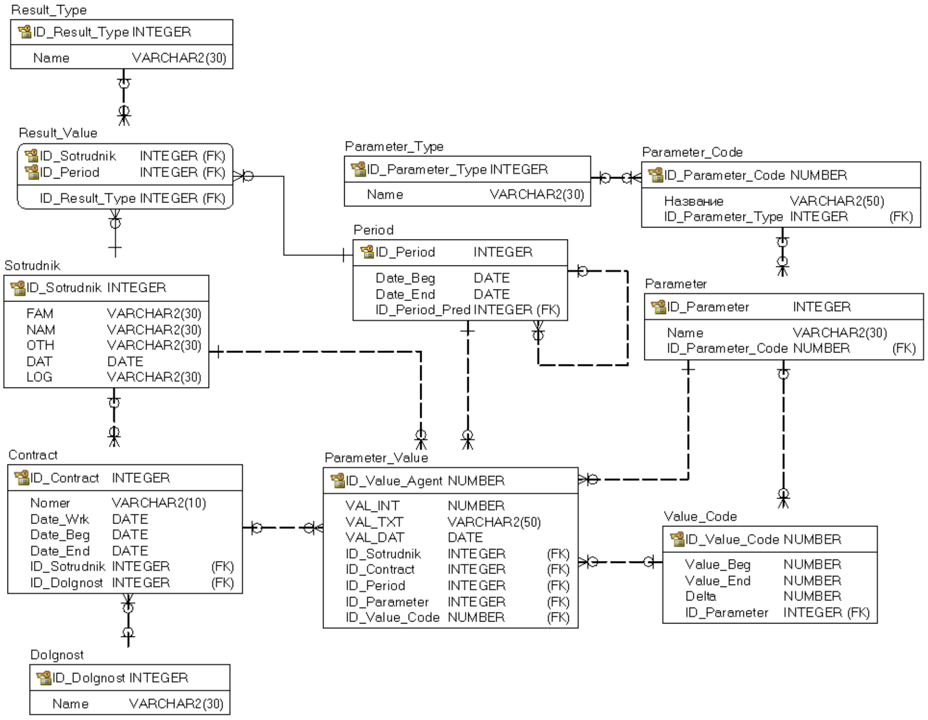

Fig. 2. – ER diagram (single data storage)

We will use the fuzzy inference procedure (figure 3) for evaluation of an individual activity. We input employee's information in the form of set of its characteristics (the values of the linguistic variables), then the output is an information about the extent of his belonging to the insider status.

The procedure is based on the algorithm Mamdani-Zadeh of the fuzzy inference. The construction of membership functions and the compilation of the rule base are carried out by an expert (or group of the experts) and are easily adjusted depending on the circumstances. The rule base can be stored in a separate database schema and it is constantly updated.

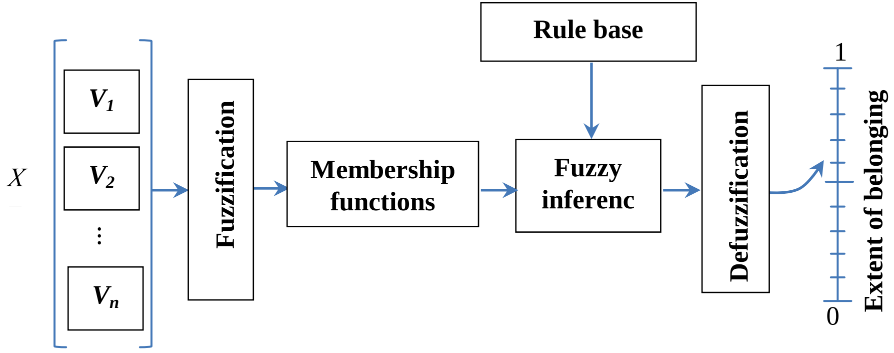

Fig. 3. – Procedure of fuzzy inference

The results of the analysis of activity of employees can be viewed in appropriate form of the system. Appropriate forms were developed for entering new characteristics and editing present ones of employees' activity (entity "Parameter", "Parameter_Code" and "Parameter_Type", see figure 2), membership functions, and rules of the knowledge base. Appropriate databases were developed for membership functions and rules of the knowledge base. This approach enables to take into account the peculiarities of the different companies' activities. Set of characteristics by themselves, characteristic sets, membership functions and rules in the knowledge base can be issues of sharing and discussions by the specialists.

This system will allow in real time to assess the state of data security in the CIS and the activities of employees working with sensitive data. In the case of appearing of the insider attacks marks, the system will automatically block the action of a potential insider and inform the corporate management about the danger. It should be noted that the system does not require maintenance by highly qualified specialists because it was created and customized by the expert for the specific company. Hence database of membership functions and rules of the knowledge base can be used independently from the highly skilled professionals.

References

1. **Zimmermann HJ.** Fuzzy Set Theory and its Applications. 3rd ed., Dordrecht: Kluwer Academic Publishers, 1996.
2. **Cappelli DM, Moore AP and Trzeciak RF.** The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Pearson Education, 2012.
3. CERT Insider Threat Center. Pattern-Based Design of Insider Threat Programs (CMU/SEI-2014-TN-024). Software Engineering Institute, Carnegie Mellon University, 2014.