UDC 004.942:004.056.53

A.I. Mikhalyov, Yu.O. Kaliberda

DEFINITION OF IDS REQUIREMENTS ON THE BASIS OF THE MODEL WITH ARTIFICIAL IMMUNITY IN NETWORK SECURITY SYSTEMS

Annotation. *It is suggested to use the components of network traffic to recognize abnormal activity in the network, which can be divided into two parts: static and dynamic. The static component of the traffic is the information transmitted. The dynamic component of the traffic is a sequence of time intervals corresponding to the transmission times of the packets and the waiting state of the communication link.*

Key words: *artificial immune system, clonal selection, negative selection, safety*

Formulation of the problem

The IDS (Intrusion Detection System) software products are increasingly becoming a necessary complement to the network security infrastructure. In addition to firewalls, which work on the basis of security policy, IDS serve as mechanisms for monitoring and observation suspicious program activity. They can detect attacking software agents that have bypassed the firewall and issue a report to the administrator, who can take further steps to prevent an attack.

Main part

IDS is a process of identifying anomalies in computer networks. In practice IDS includes the following types of anomalies:

Unauthorized actions of employees;

Recognition of external factors that contribute to the theft of information;

Intrusion and obtaining privileged access to enterprise computing resources;

Detection of abnormal operation of equipment and software;

Detection of active hacker attacks.

The goal is to more effectively solve the recognition problem using the algorithm of artificial immunity. The model of such an analyzer consists of the following modules:

Monitoring module. The function of this module is to monitor network traffic and create an event log;

 ISSN 1562-9945

Comparison module. This module receives logs from the monitoring module and compares them. The result of the work will be a lot of identical fragments (signs);

The repository. This module stores all the grouped event logs according to a certain characteristic;

Decision making module. Determines if there is an abnormal network traffic at the time.

It is known [1] that the problem of detecting anomalies in computer networks is very laborious, since there are many network protocols that operate at different levels of the OSI model (IP, ICMP, SNMP, TCP, UDP, HTTP, ARP). In this case, each of the protocols has a number of vulnerabilities. For example, different computers have different operating systems and sets of software, which have errors and backdoors, which allow you to access the network from somewhere outside. These factors together generate a huge number of very diverse methods of obtaining unauthorized access to the network and computing resources of the enterprise.

For each species and subspecies of anomalies, there are signs that can be detected by one or other of the detectors. When detectors are triggered, an analysis takes place: which of the groups of detectors have worked and what in aggregate can they say about this type of anomaly. The detector carries information about the protocol, service or pattern of behavior on the network, and so on. To obtain the best result, it is necessary to generate detectors in such a way that the minimum number of detectors can detect the maximum number of anomalies.

The basic idea of IDS based on artificial immunity is the definition of a *non-self* template from a set of known *self*-patterns. Parameters for detectors can be written as a finite number of lines that characterize different types of anomalies. The total number of varieties of strings sets the set:

$$X \in \{0,...,n\}.$$

The set X consists of subsets of *self* and *non-self* $S \subset X$, $N \subset X$, such that $S \cup N = X$ and $S \cap N = 0$. In IDS, unsafe templates represent an IP packet from the attacking computer, in turn, a secure template for the normal functioning of the network node. The task of the detection algorithm is to classify the input string $I \in X$ into a *self* / *non-self*

template. The set of detectors D with which rows are to be compared, the similarity function $f(I, D)$, and some threshold ε that determines whether the string is self or non-self $compare(D, I, f, \varepsilon)$.

$$f(I,Di)<1-\varepsilon=non\text{-}self,$$

$$f(I,Di)\geq 1-\varepsilon=self.$$

To recognize abnormal activity in the network, it is necessary to identify a list of characteristics by which this recognition will be performed. Network traffic consists of two components: static and dynamic. The static component of the traffic is the transmitted information, i.e. The sequence of packets and the data contained in them. The dynamic component of the traffic is a sequence of time intervals corresponding to the transmission times of the packets and the waiting state of the communication link. The following factors should be taken into account:

The random nature of synthesized delays;

Logicality of the attacker's actions;

Multi scenario attack.

Select the types of delays to be modeled:

The end-to-end packet propagation delay is the time that a packet is transferred from one point on the computer network to another. It can be described by the sum of a deterministic quantity and a random variable with a gamma distribution;

The time the server executes the request is a deterministic value determined by the algorithm of the server software;

Software delay is a deterministic value, which is determined by the algorithm of the client program;

Delay command input - a random delay, determined by the time required by the attacker or the user to enter the next command or request. We will consider the delay value as a normal random variable with mathematical expectation and variance, depending on the length of the input command and the average speed of text typing by the user (attacker).

The delay in evaluating the result is a random delay, related, first, to the amount of text that should be read or viewed by the user or the attacker, and, secondly, with the need to perform any calculations. Let us take this delay, distributed according to the normal law.

Thus, it is necessary to model five different types of delays, three of which are random variables. The main task is to collect the most complete set of significant features. In this case, as parameters for the detectors, we will use the value of the fields of the structure of the corresponding protocol packet.

The IDS structure should be distributed with a large number of connections between nodes and without centralized management, because the failure of the central node paralyzes the entire system. However, the logical structures of the system must proportionally distribute the functioning of the system. It should be taken into account that all nodes exchange service information over encrypted channels to report the presence of an anomaly in the network and prevent its propagation in the network.

There are three logical levels: system, network, local.

At the system level:

- Monitors the overall state of the system;
- Identifies and localizes problems;
- Provides extended information to an expert;

At the network level:

- Tracks traffic between network nodes;
- Exchanges data with nodes to report their status (sends a message to the system level).

At the local level:

- Is responsible for detecting anomalies;
- Reacts to an anomaly;
- Generates known anomalies for system learning.

The main processes that occur in the system are:

- Generation of non-self packages;
- Detecting anomalies;
- Monitoring;
- Interaction with neighboring nodes;
- Classification;
- An attempt to counteract the detected anomalies;
- Restoring the network to normal mode;
- Alerting the expert about the detected anomalies.

References:

1. Mikhalyov A.I., Kaliberda Yu.O. Application of artificial immune systems for the detection of anomalies in network traffic / / International scientific conference of the system of telecommunications and information technology (ISDMIT` 2006) 2006 (2). - P. 215-217.
2. Mikhalyov A.I., Kaliberda Yu.O. Mathematical model of the immune response to intrusion into the computer network. // System technologies. Regional intercollegiate collection of scientific works. - Issue 3 (56). - Volume 2. - Dnepropetrovsk, 2008. - P.175-178.