METHOD OF CONSTRUCTING SECURITY MODELS OF COMPUTER SYSTEMS

Alekseev, Viktor M., *Moscow State University of Railway Engineering (MIIT), Moscow, Russia.*

ABSTRACT

The article considers issues related to the construction of monitoring systems that provide detection of threats in the information environment. In particular, the recognition method for implementing models of analyzers in the zone of a given space of trusted and possible untrusted information traffic routes.

Keywords: information security, isolated software environment, hidden channels, monitoring of subjects.

Background. The urgency of the problems of building the model of information security is obvious. A lot of publications are devoted to this issue. There is a constant struggle between companies defending their intellectual development, groups of people who try to take them by unfair methods. Since data storage, information exchange is carried out using network technologies, it becomes possible to steal critical information. Public infrastructure facilities, including those belonging to the transport industry, are subject to information attacks.

In this text, the task is to justify and evaluate the use of recognition methods for the implementation of models of threat analyzers. The essence of the approach is that any process of the generation of information and its transmission over the computer network should be strictly regulated. The problem is to implement a system that recognizes trusted routes in the information system by a set of different characteristics. The training of such a recognizing system can take place with or without a teacher. In this case, we describe an approach to solving the classical recognition problem using a given space of trusted and possible untrusted routes. The decisive rules that ensure the recognition of the correctness of information movement along trusted routes should be based on the use of regulatory documents of the organization for which the system is being implemented.

Objective. The objective of the author is to consider a method of constructing security models of computer systems.

Methods. The author uses general scientific and engineering method, comparative analysis, mathematical calculations.

Results. Recognizing systems work only on the basis of signs. A feature space is generated using built-in agents that are installed on network infrastructure objects: switches, access points, routers, firewalls, servers and personal computers.

The signs are formed taking into account:

– numerical parameters (the number of data transferred via various protocols, the CPU load, the number of files, and so on);

– categorical parameters (types of protocols, file names, open ports, etc.);

– non-standard parameters (packet delay time, hash prints of login and password, biometric parameters, etc.).

Based on the administrative security documents for each unit, trusted routes in the information system are established that determine the movement of information.

To implement the model, it is suggested to use the coordinates of the network infrastructure objects specified in the form of a coordinate model. This principle allows to move to a description using numerical coordinates instead of letter values of objects or subjects. New opportunities are opened for adding additional objects to the model (for example, identifying hidden information leakage channels), expanding the functionality of the information system (say, creating special hardware for storing information), and reconstructing the infrastructure of the information system (changing the network structure of the enterprise).

The base of decisive rules in the recognition system is realized on the basis of constructing a model consisting of objects, subjects and graphs connecting them. The resulting decision rules represent sets of chains on which information moves in the controlled system. And each object has certain coordinates assigned to it in the coordinate model. As noted above, the decisive rules must be formed on the basis of various characteristics: allowed protocols, ports, authentication sign (from the kerberos server, biometric features) and attributes of the coordinates of the objects of the network, on which the information moves, as well as geoinformation characteristics of the subjects admitted to the system. Each characteristic has an assigned numerical equivalent.

The decisive rules determine the trusted traffic routes of information on the computer network. In this case, there may be cases:

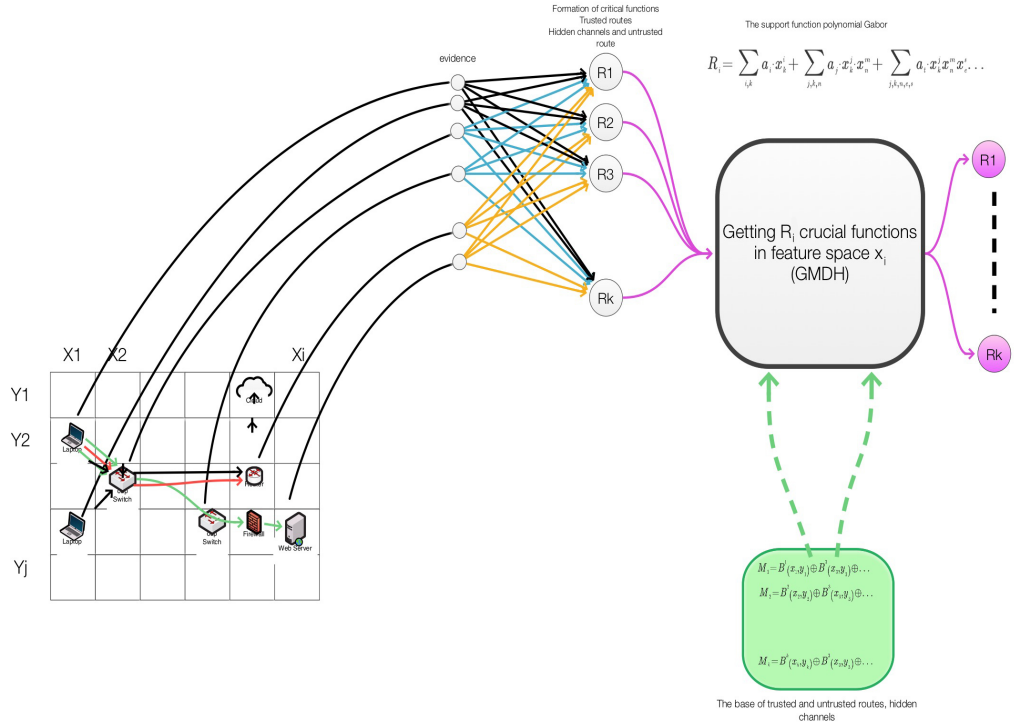
– loss of information due to the emergence of queues on objects (switches, routers, access points);

– Illegal sending of information on an untrusted route (the subject tries to illegally send information);

– hidden channels of information transfer (legally installed applications send personal data from the workstations of users' computers).

Let's consider methods of obtaining decision rules. Obtaining decisive rules is the most crucial step in implementing the security model of a controlled system. Such rules are obtained using the method of self-organization – group accounting of arguments [1]. Pic. 1 shows a graphical interpretation of the method using a multi-row perceptron. The system considers possible options for information movement, prescribed in administrative documents (the base of trusted and untrusted routes, hidden channels). Here, there are also cases involving loss of information, untrusted routes, hidden channels, and other leakage options.

In the implementation of the decisive rules, geo-information features of subjects and objects that can be admitted to work in the system



Pic. 1. Construction of decision rules.

participate. The entire network is represented by a grid model, which defines the coordinates of the installation of objects (switches, routers, servers and other equipment). Moreover, the network detailing causes the depth of the threat analysis in the network. The decisive rules are linguistic chains constructed according to the network structure model.

The Gabor polynomial is chosen as the supporting function:

$$R = \sum_{i,k} a_i \times x_k^i + \sum_{j,k,n,m} a_j \times x_k^j \times x_n^m + \\ + \sum_{j,k,n,m,e,s} a_j \times x_k^j \times x_n^m \times x_e^s. \quad (1)$$

The central states of objects included in the database of routes are also involved in obtaining decisive rules. We believe that if the route is correctly implemented, the packet does not deviate from the specified route and moves along one of the routes specified in the database. In this case, a sequential route of information movement with the participation of the relevant objects is realized. At each B_i object, the correspondence of the information contained in the packet, the specified route, must be checked. Implementing this condition in a decisive function is possible with the use of the Gabor polynomial. The coefficients are calculated on a multi-row perceptron. Let x_{i+1} and the central value is 1. The central value for attribute x_{i+1} is formed from the trusted routes database. From the Gabor polynomial for two signs x_i and x_{i+1} it follows:

$$R = a_0 \times x_i + a_1 \times x_{i+1} + a_2 \times x_i \times x_{i+1} + \\ + a_3 \times x_i^2 + a_4 \times x_{i+1}^2 + \ldots + . \quad (2)$$

The terms in equation (2) with coefficients a_2, a_3 and a_4 represent the square of the difference

$$R = (x_i - x_{i+1})^2, \quad (3)$$

at certain values of coefficients.

The attribute x_i takes one of the values from the set M_{pr} (the correspondence of the numeric value 0 is the http protocol, 1 is dhcp, 2 is sip, and so on). The x_i attribute is generated using agents installed on objects. The output R and the characteristic values are given in Table 1.

Substituting the values of the characteristics and output of the model in equation (2), we obtain an overdetermined system, which we solve by the Gauss method [1, 2] for redefined systems of equations:

$$[a_k] = [R] \times [x_{ij}]^T \times \left([x_{ij}] \times [x_{ij}]^T \right)^{-1}. \quad (4)$$

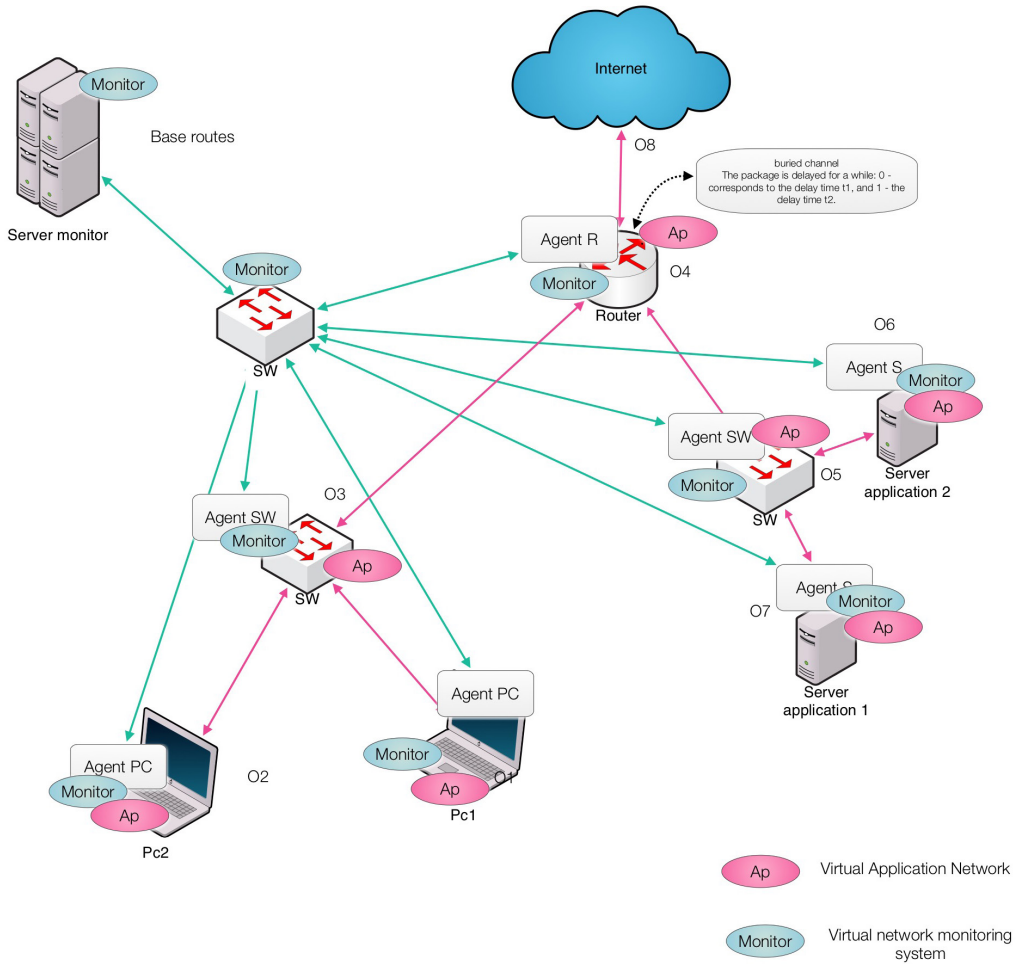
In case of forming a route on an object with additional characteristics, the general description of the Gabor polynomial will look like:

$$R = a_0 \times x_i + a_1 \times x_{i+1} + a_2 \times x_i \times x_{i+1} + a_3 \times x_i^2 + \\ + a_4 \times x_{i+1}^2 + a_5 \times x_j^2 + a_6 \times x_{j+1}^2 + a_7 \times x_j \times x_{j+1}. \quad (5)$$

From the above formula (5) it follows that for two characteristics the decisive rules will have the form:

$$R = (x_i - x_{i+1})^2 + (x_j - x_{j+1})^2, \quad (6)$$

For each B_i object, the decisive rules R_i are constructed in accordance with the specified trusted route. If several B_i objects participate in the route, then all decisive rules are formed into a single one describing the passage of the packet



Pic. 2. Monitoring network (ISE) with in-built agents.

$$R_{B1} = \sum_i \left(x_i - x^*_{i,B1}\right)^2, \text{ for the object } B_1, \quad (7)$$

$$R_{B2} = \sum_i \left(x_i - x^*_{i,B2}\right)^2, \text{ for the object } B_2, \quad (8)$$

$$R_{Bj} = \sum_i \left(x_i - x^*_{i,Bj}\right)^2, \text{ for the object } B_j \quad (9)$$

and converted to a formula for the trusted route M_k:

$$R_{M_k} = \sum_i \left(x_i - x^*_{i,B1}\right)^2 + \sum_i \left(x_i - x^*_{i,B2}\right)^2 + \ldots$$

$$+ \sum_i \left(x_i - x^*_{i,Bj}\right)^2, \quad (10)$$

Table 1

The values of the outputs of R and signs

X_i	X_{i+1}	R_{output}
0	1	1
1	1	0
2	1	1
3	1	4
4	1	9
5	1	16

where i = 1, n is a number of set signs in the monitoring system, formed by the agents.

The determination of belonging of the real information flow to one of the decisive rules takes place in real time by collecting information from embedded agents in the infrastructure objects (see Pic. 2). The information monitoring network is virtually separated from the monitored network and must meet the requirements of the lemma (the basic theorem of the isolated software environment ISE) [3, 4].

Lemma. If, from the time t_0, *only the generation of subjects with source invariance control is effective in ISE, and all the generations are absolutely correct relative to each other, as are the existence of subjects (including security monitoring of objects and subjects), then at any time* $t>t_0$, *the software environment remains ISE.*

By the condition of the lemma, in the software environment, there may exist flows that change the state of objects that are not associated at that time with any subject. If the object with the changed state is not a source for generating the subject, then the set of ISE subjects is not extensible, otherwise (the modified object is the source for generating the subject), by the condition of the theorem

(generation of the subject with control), the generation of the subject is impossible. Thus, at any time $t>t_0$, the software environment remains the ISE medium. The emergence of the information flow is done by the subject by initializing the application, which is linked according to the specified protocol to the application server. For the technical implementation of the security monitoring model, it is required:

• observance of the correctness of subjects by using the virtual part in the local network VLAN, sharing resources: objects and subjects within the network, and in the external environment using VPN (ip-sec protocol);

• monotony of the rules implementation – unchanging the rules of the application functionality in the network;

• implementation of monitoring of the security of objects and subjects with mandatory use of signs of identification through means built into the OS.

The processing must take place on each model of the object B_i as the package moves forward. The most difficult moment is connected with the loss of the packet or its queue, when the switch is overloaded and the reduction model of randomly selected packets is used, that is, removal. In this case, the packet is lost, and therefore the decisive rule will give the result that the packet does not follow any of the trusted routes. So, it is necessary to include decisive rules that will reflect this specific network. Packet buffering works on all switches, routers, firewalls and other network devices. The package can be deleted or delayed for the duration of the priority pass. That is, it takes some time to track the package, and this requires «fixing» the decisive rule that tracks a certain trusted route after it reaches the network infrastructure object.

The case of hidden channels is different in that the packet starts to move along a trusted route (see Pic. 2). But the peculiarity is that the packet is delayed for some time: 0 – corresponds to the delay time t_1, and 1 – the delay time t_2. The agent of the hidden channel produces a delay, at first glance innocuous, thereby transmitting sensitive information. Typically, this is done on the end device of the router, which again shows that the analyzers should contain a model that allows to track time delays.

The packet arrives at the generated rules for monitoring trusted routes on the network, untrusted routes and hidden channels. The signs formed by agents come to the whole set of decisive rules. Agents form a space for the characteristics of the packet on the network, which enter the decisive rules. The decisive rules give values, formed depending on the path of the packets:

– agent of the object 1: signs x_i –> decisive rules of the object 1 of all routes;

– agent of the object 2: signs x_i –> decisive rules of the object 2 of all routes;

– agent of the object n: signs x_i –> decisive rules of the object n of all routes.

A decisive rule that takes a minimum value or is equal to zero, shows which route the given packet, formed by the application P_{ri}, is passing. The packet route is compared with the trusted route of P_{ri} application. If the value of R_{Mk} is zero and matches the given value in the base of the decisive rules, then there is no threat. In the case of the inequality $R_{Mk} \neq 0$, decisive rules with a minimum numerical value are sought, then they are compared with the base routes M and a conclusion is made about the occurrence or absence of a threat under the index j:

$$min\left(R_{M_k}\right) \rightarrow \forall k, \left(R_{M_k} \rightarrow M_j\right); j \in \{1, k\}. \qquad (11)$$

The process of correctness of the work of decisive rules is evaluated by the reliability of P_d control and depends on the errors of the first P_1 and the second kind P_2, caused by the resulting inaccuracies in the formation of attributes by agents at the objects due to program errors and other factors. Reliability is determined by: $P_d = 1 - P_1 - P_2$.

Conclusions. The use of recognition methods for the implementation of security models is a breakthrough direction in the implementation of methods for ensuring information security in computer systems. The application of a coordinate model to the representation of infrastructure objects that provides the use of numerical coordinates of objects and subjects in decision rules provides the possibility of implementing information in the model of trusted traffic routes, as well as formalization of hidden transmission channels, untrusted information transmission channels and other new aspects of implementing security models at the interaction level of subjects and objects of network infrastructure.

An important advantage of the approach is that it does not require large computing power, it is easier to implement systems that operate in real time and control the processes of information transfer, improve the level of security and prevent information leakage.

REFERENCES

1. Ivakhnenko, A. G. Decision-making on the basis of self-organization [*Prinjatie reshenij na osnove samoorganizacii*]. Moscow, Sovetskoe radio publ., 1976, 325 p.

2. Ivakhnenko, A. G. Inductive method of self-organization of models of complex systems [*Induktivnyj metod samoorganizacii modelej slozhnyh system*]. Kiev, Naukova dumka publ., 1982, 246 p.

3. Devyanin, P. N. Models of computer systems security [*Modeli bezopasnosti komp'juternyh system*]. Moscow, Gorjachaja linija-Telekom publ., 2013, 338 p.

4. Alekseev, V. M., Alekseev, V. V. Model of information interaction of services in the IT system of high-speed transport [*Model' informacionnogo vzaimodejstvija servisov v IT-sisteme vysokoskorostnogo transporta*]. *Transport Urala*, 2012, Iss. 3, pp. 43–48.

Information about the author:
Alekseev, Viktor M. – D.Sc. (Eng.), professor of the department of Control and information security of Moscow State University of Railway Engineering (MIIT), Moscow, Russia, avm@niit-miit.ru.

Article received 03.10.2016, accepted 22.12.2016.