ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 72
IV International Research Conference "Information Technologies in Science, Management, Social Sphere and Medicine" (ITSMSSM 2017)

A Fault-tolerant Two-tier Pattern Of Secure Access 'Connecting Node'

Vladimir S. Kolomoitcev, Vladimir A. Bogatyrev
Department of Computation Technologies
ITMO University
St.Peterburg, Russia
dek-s-kornis@yandex.ru, vladimir.bogatyrev@gmail.com

***Abstract*—The purpose of this paper is to study a fault-tolerant system of secure access to the corporate network and to select the options for allocating resources of the server for the system's information protection software that is installed on it, given that the conflicting requirements, arising in this case, are met. A two-tier pattern of access, including two groups of routers and a group of servers with the software that implements the functions of secure access to information, is proposed to be the basis for designing the protection system. The considered technical solutions were analyzed for effectiveness using the mathematical model that was developed to estimate the average time of the request in the system, depending on the means of information protection involved. An example of calculating the average time of the request in the system, with two types of software for information protection (firewall and antivirus) installed on the server, was given. An example of calculating the degree of information security computing system, with different number of used software for information protection, was given too. Options for allocating resources of the server to ensure the operation of the existing bundle of software means for information security were examined and their effectiveness was assessed.**

Keywords—Information security; software; computer systems; means of protection; pattern of access; information protection; firewalls

I. INTRODUCTION

The effectiveness of a computer system (CS) and network is largely determined by the organization of the system of fault-tolerant secure access to its resources. The design process of both - the protection system and the CS on the whole - involves achieving the compromise over its cost, reliability, security, and performance for the used software and hardware means [1], [2], [3].

System protection of the CS provide for opposition: unauthorized access, malicious software (including viruses), damage or theft of information, etc. Software and hardware that performs tasks for the protection can implement functions of firewalls, antivirus means, cryptographic locks, secure storage [4].

The purpose of this paper is to study the search for rational options of a fault-tolerant pattern of secure access ‘Connecting node’, providing the highest possible degree of information security of CS while limiting financial and computing resources for its design.

In order to achieve this purpose in the work is the study of options of designing a fault-tolerant system of secure access ‘Connecting node’ and to select the options for allocating resources of the server for the system's information protection software that is installed on it, given that the conflicting requirements, arising in this case, are met.

II. THE PATTERN OF SECURE ACCESS 'CONNECTING NODE'

The pattern of secure access 'Connecting node' is based on the standard pattern of access 'Direct connection', which uses a serial connection of all key elements and components of a CS between each other [4], [5]. For high quality and uninterrupted operation of the CS, its key elements are usually reserved. The structure of the common pattern of secure access ‘Connecting node’ includes a group of servers that accommodate most software for supporting the process of information protection of CS and two groups of routers intended for connecting the external network, the group of servers, and the end nodes of the CS with each other. Fig. 1 shows a model of the pattern of secure access 'Connecting node'.

Data coming from the external network in the CS arrive at the first group of routers in the beginning and, if not corrupted, are sent to the group of servers for the analysis for the presence of any malicious content. A bundle of software that resides on servers of the group is selected depending on the purpose of the CS, financial constraints on the organization of its design, and the potential information security threats.

After analyzing the received data for potential threats, a server of the group forwards the data to the second group of routers, which are to send them to the desired end node of the CS. End nodes of the CS have individual software to protect information (for example, a personal antivirus, with an internal firewall). That software is designed to deal with specific threats for each node of the CS.

Two groups of routers are needed to increase information security of the CS. They allow reducing significantly the chances of unauthorized access to the terminal nodes of the CS from an external attacker [5], [6].

The pattern of secure access 'Connecting node' can be expanded with additional hardware protection (firewalls, intrusion detection system, kryptosysteme, etc.) which are located before the first group of routers (at the entrance to the corporate network) and immediately after it. This is possible due to the fact that the basis for its design is a pattern of secure access 'Direct connection'. This step allows reducing the computational load on the server group, and improving the degree of information security of the CS.

However, it is worth considering that a pattern of secure access 'Connecting node' in first place focused on software that ensures information security of a CS. Therefore, most part of all means that provides the information security of the CS will be located on the server group.

In this work, we will adhere to the common view of a pattern of secure access 'Connecting node'.

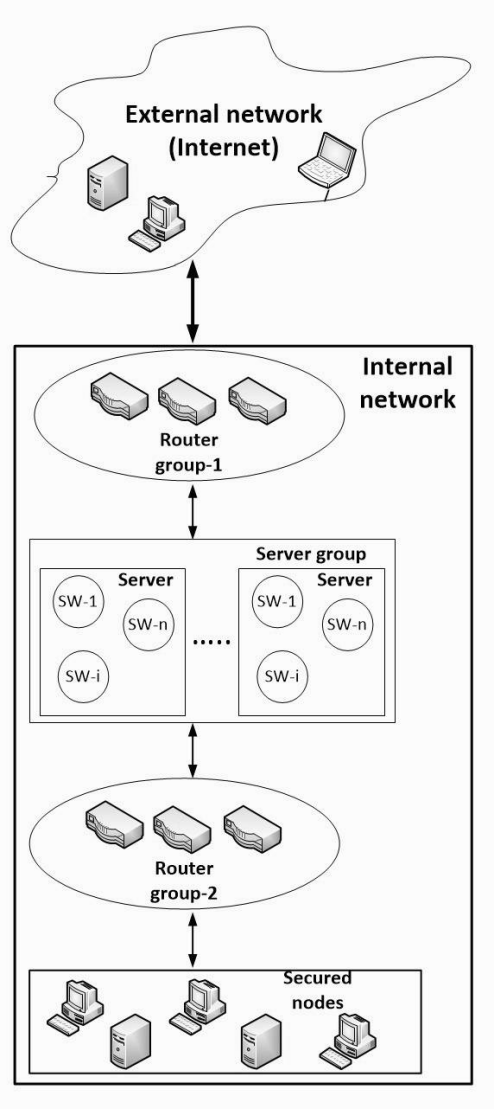

Fig. 1. The pattern of secure access 'Connecting node'

III. Selection and Optimization of Options of the Pattern of Secure Access

The process of selecting and optimizing design alternatives for the pattern of access 'Connecting node' means determining the rate of redundancy for nodes in each group by which the minimum average residence time of the request in the system T_s is achieved (ARTRS), taking into account the constraints on the costs of implementing the system C [7], [8], [9], [10].

The cost of implementing the system of protection is equal to:

$$C = c_1 \cdot N + c_0 \cdot \sum_i m_i ,$$

where c_0, c_1 is the cost of routers and servers, N is the number of servers, and m_i – the number of routers in the i-th group.

Let us assume that the total number of resources in the server for the implementation of information security has a limit is Q. To support of a normal level of functionality (performance) of their work, the means of protection require the certain amount of resources, as shown in (1):

$$\sum_i n_i \cdot q_i \le Q , \quad (1)$$

where q_i is the cost of server resources to maintain full operation of the i-th software, n_i is the number of copies (in case of redundancy) for the i-th software; $q_i \ge r_i$, where r_i is the minimum amount of server resources required to operate the i–th software. In this case, in the conditions of limited resources, a general reduction in potential performance for the total security software will be:

$$k_i = k = Q / \sum_i q_i \cdot n_i . \quad (2)$$

When differentiating resources for different security software, reducing the potential level of possible performance of the i–th software s defined as:

$$k_i = u_i / q_i \cdot n_i \quad (3)$$

Here, u_i is the number of server resources allocated for the work of the i-th software.

Each node in the access patterns introduces a queueing system of type M/M/1 with the infinite queue. When distributing the flow of requests for processing to n nodes, ARTRS for each of the nodes can be calculated as:

$$T = \nu / (1 - \nu \cdot \lambda / n) \quad (4)$$

Here v is the average service time of the request in the node; λ is the intensity of the request flow.

For the system of serially nodes, the total ARTRS can be determined as:

$$T_O = \sum_i T_i \quad (5)$$

Optimizing the system of protection implies finding the distribution of the number of nodes of each type, which provides the minimum ARTRS, assuming that there are cost constraints C on the implementation of the system and the conditions of stationarity of the maintenance mode are met [11], [12], [13], [14], [15].

After the input flow has been filtered in the first group of routers, its intensity of the flow of requests coming to the group of servers turns out to be lower than before. Similarly, after the malicious content has been removed with the server software, the resulting flow of requests that arrives at the second group of routers proves to be even less.

In this study, we assume that the routers and the software that resides on the servers have so called common areas, which are to detect and eliminate threats to information security. As a result, some of the threats can be detected and eliminated by several types of the software (or other security feature consisting of patterns of access) [16].

Thus, using (4) and (5), ARTRS for this system, consisting of two groups of routers and the two types of software (SW-1 and SW-2) located on each server is calculated as:

$$T_s = \frac{V}{1-Y/m_1} + \frac{\nu_1'}{1-d_1 \cdot F_1} + \frac{\nu_2'}{1-d_2 \cdot F_2} + \frac{V}{1-d_3 \cdot Y/m_2} \quad (6)$$

Here $\nu_i' = \nu_i \cdot k_i$; $Y = \lambda \cdot V$; $F_i = \lambda \cdot \nu_i' / N \cdot n_i$;

$d_1 = (1 - L \cdot W \cdot A_0 \cdot p_0)$;

$d_2 = 1 - L \cdot W \cdot (p_1 \cdot (A_1 - l_{10}) + p_0 \cdot (A_0 - l_{10}) + l_{10} \cdot (1 - \overline{p}_0 \cdot \overline{p}_1))$;

$d_3 = 1 - L \cdot W \cdot (p_1 \cdot S_1 + (1 - \overline{p}_0) \cdot R_e + p_2 \cdot S_2 +$
$+ (l_{10} - l_{00}) \cdot (1 - \overline{p}_0 \cdot \overline{p}_1) + (l_{20} - l_{00}) \cdot (1 - \overline{p}_0 \cdot \overline{p}_2) +$
$+ (l_{21} - l_{00}) \cdot (1 - \overline{p}_1 \cdot \overline{p}_2) + l_{00} \cdot (1 - \overline{p}_0 \cdot \overline{p}_1 \cdot \overline{p}_2))$,

where $R_e = (A_0 - l_{20} - l_{10} + l_{00})$; $S_1 = (A_1 - l_{21} - l_{10} + l_{00})$;
$S_2 = A_2 - l_{21} - l_{20} + l_{00}$,

and A_0, A_1, A_2 is the proportion of the threats (errors) from the set of threats detected by the router with probability p_0, SW-1 with probability p_1 and SW-2 with probability p_2; l_{00} is the proportion of the threats from the set of threats where errors can be detected and eliminated by either the router and SW-1 and SW-2 at the same time; l_{10} is the overlapping area for the router and SW-1; l_{20} is the overlapping area for the router and SW-2; l_{21} is the overlapping area for the SW-1 and SW-2; $L = \lambda_T / \lambda$ is the proportion of the threats in data flow, where λ_T is the intensity of flow of threats and λ is the intensity of total input data flow (including threats); $W = |E| / |H|$, where $|E|$ is the cardinal number of the set E (the set of threats that can detect and eliminate the means as part of a system of information protection), $|H|$ is the cardinal number of the set H (the set of information security threats, which need to be addressed in the framework of a specific CS).

We present the results of the calculation: $A_0 = 25\%$; $A_1 = 50\%$; $A_2 = 80\%$; $p_0 = 0.9$; $p_1 = 0.925$; $p_2 = 0.925$; $\lambda = 50\ c^{-1}$; $l_{00} = 22{,}5\%$; $l_{10} = 22{,}5\%$; $l_{20} = 25\%$; $l_{21} = 30\%$; $W = 1$; $L = 0.4$; $V_M = 0.015$ s; $\nu_1 = 0.025$ s; $\nu_2 = 0.05$ s; $c_0 = 15\ cu$; $c_1 = 90\ cu$ and limitation of funds for system design $C = 400\ cu$.

If there are enough server resources to support the full-fledged operation of SW-1 and SW-2 with $q_1 = 35$, $r_1 = 20$, $q_2 = 65$, $r_2 = 30$ and $Q = 100$, the minimum ARTRS is $T_s = 0.185$ s. Otherwise, with $q_1 = 40$, $r_1 = 20$, $q_2 = 70$, $r_2 = 35$ and $Q = 100$, when the performance degradation for SW-1 is allowed, the minimum ARTRS is $T_{s1.1} = 0.204$ s, and $T_{s1.2} = 0.224\ s$, when the performance degradation for SW-2 is allowed. In the second case, when both software tools are used at the same level of performance $T_{s2} = 0.214\ s$.

The obtained results show that depending on the chosen option of resource allocation among the server software, the minimum ARTRS can take different values.

The degree of information security, provided by the pattern of secure access 'Connection node', rate. Therefore, the probability of detection and elimination of threats to information security system (7), we calculate as [4], [16], [17]:

$$P_S = W \cdot \sum_{i=1}^{K} (l_i \cdot p_i + \sum_{j=1}^{j<i} (l_{ji} \cdot (1 - \overline{p}_i \cdot \overline{p}_j) +$$
$$+ \sum_{q=1}^{q<j} (l_{qji} \cdot (1 - \overline{p}_i \cdot \overline{p}_j \cdot \overline{p}_q) + \mathrm{K} + \quad (7)$$
$$+ \sum_{m=1}^{m<t} (l_{mt\ldots i} \cdot (1 - \overline{p}_i \cdot \overline{p}_j \cdot \ldots \overline{p}_m))\mathrm{K})$$

Here K is the number of means of protection of information used in a computing system; p_i is the probability of detection and elimination of threats to the i-th elements (means) of the system of information protection; l_i is the proportion of threats from the set defined only by the i-th element of the information security system consisting of K elements (means); $l_{q..i}$ is the proportion of threats from the set defined only by elements of i to q used in the system of information protection, consisting of K elements; $\overline{p}_i = (1 - p_i)$; $W = |E| / |H|$.

The degree of information security provided by pattern of secure access depends on server resources (capability). We have to solve the problem of distribution of resources among all the available server software (thereby maintaining the highest possible degree of information security) or disable some of them (thereby reducing the degree of information security of CS in certain areas), when resources are limited.

So, for the previously considered example of the calculation, for: $A_0 = 25\%$; $A_1 = 50\%$; $A_2 = 80\%$; $p_0 = 0.9$; $p_1 = 0.925$; $p_2 = 0.925$; $l_{00} = 22.5\%$; $l_{10} = 22.5\%$; $l_{20} = 25\%$;

$l_{21} = 30\%$; $W = 1$, calculations established that the degree of information security while using SW-1 and SW-2, in the system of protection, we get: $Ps = 0.9486$, when we use on the server only SW-1: $Ps = 0.5004$, when we use on the server only SW-2: $Ps = 0.7569$.

As we can see from the obtained estimates provide the degree of information security (7), depending on the software used for information security, which is located on the server, the degree of information security of the CS (probability of detection and elimination of a particular threat) can vary considerably. As a result, subject to the limitation of computing resources of the server, the solution of the optimization problem for obtaining the minimum ARTRS when the maximum degree of information security of CS is necessary.

IV. Conclusion

We proposed a two-tier pattern of secure access 'Connecting node', comprising two groups of routers and a group of servers, with the software implementing functions of secure access to information.

Based on the proposed mathematical model, an example calculation of the average time of request in the system using two types of software of protection of information residing on the server was shown.

The efficiency of the considered options of implementation of the pattern of secure access 'Connecting node' was evaluated.

We have shown the influence of the distribution of computing resources of servers on the average residence time of the request in the system and provide the degree of information security of the computer system.

References

[1] T. I. Aliev,, "The synthesis of service discipline in systems with limits", in: DCCN 2015. CCIS, vol. 601, pp. 151–156. Springer, Heidelberg (2016).

[2] Kopetz H., "Real-Time Systems: Design Principles for Distributed Embedded Applications", Springer, pp. 396, 2011.

[3] V.S. Kolomoitcev, "A comparative analysis of approaches to organizing of secure connection of the corporate network nodes to the public network", Cybernetics and Programming, N. 2, pp. 46-58, 2015.

[4] V.S. Kolomoitcev, "Choice of option for implementation of the multilevel secure access to the external net-work", Scientific and Technical Journal of Information Technologies, Mechanics and Optics, vol 16, №. 1, pp. 115–121, 2016.

[5] V.S. Kolomoitcev, V.A. Bogatyrev, "The fault-tolerant structure of multilevel secure access to the resources of the public network", Communications in Computer and Information Science, vol 678, pp. 302-313, 2016.

[6] S.A. Arustamov, V.A. Bogatyrev, V.I. Polyakov, "Back up data transmission in real-time duplicated computer systems", Advances in Intelligent Systems and Computing, vol 451, 2016, pp. 103-109

[7] V.A. Bogatyrev, S.V. Bogatyrev, I.Y. Golubev, "Optimization and the process of task distribution between com-puter system clusters", Automatic Control and Computer Sciences, vol 46, No. 3, pp.103-111, 2012.

[8] V.A. Bogatyrev, S.A. Parshutina, N.A. Poptcova, A.V. Bogatyrev, "Efficiency of redundant service with de-struction of expired and irrelevant request copies in real-time clusters", Communications in Computer and Information Science, vol 678, pp. 337-348, 2016.

[9] V.A. Bogatyrev, "Exchange of duplicated computing complexes in fault tolerant systems", Automatic Control and Computer Sciences, vol 45, №. 5, pp. 268–276, 2011.

[10] 10. V.A. Bogatyrev, A.V. Bogatyrev, "Functional reliability of a realtime redundant computational process in cluster architecture systems", Automatic Control and Computer Sciences, vol 49, №. 1, pp. 46-56, 2015.

[11] V.A. Bogatyrev, S.A. Parshutina, "Redundant distribution of requests through the network by transferring them over multiple paths", Communications in Computer and Information Science, vol 601, pp. 199-207, 2016.

[12] V.A. Bogatyrev, S.A. Parshutina, "Efficiency of redundant multipath transmission of requests through the net-work to destination servers", Communications in Computer and Information Science, vol 678, 2016, pp. 290-301.

[13] V.A. Bogatyrev, "An interval signal method of dynamic interrupt handling with load balancing", Automatic Control and Computer Sciences, vol 34, № 6, 2000, pp. 51-57.

[14] V.A. Bogatyrev, "Protocols for dynamic distribution of requests through a bus with variable logic ring for re-ception authority transfer", Automatic Control and Computer Sciences, vol 33, №. 1, 1999, pp. 57-63.

[15] V.A. Bogatyrev "On interconnection control in redundancy of local network buses with limited availability", Engineering Simulation, vol 16, № 4, 1999, pp. 463-469.

[16] V.S. Kolomoitcev, K.U. Bodrov, A.V. Krasilnikov, "Calculating the probability of detection and removal of threats to information securityin data channels", in 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM), St. Petersburg, pp. 25-27, 2016.

[17] V.S. Kolomoitcev, V.A. Bogatyrev "Probabilistic and temporal indicators in the stage-by-stage use of information protection means", in press.