ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2013
Seria: ORGANIZACJA I ZARZĄDZANIE z. 67 Nr kol. 1900

Vadym MUKHIN
National Technical University of Ukraine "Kiev Polytechnic Institute"
Computer Systems Department

THE RATING MECHANISM FOR THE TRUSTED RELATIONSHIP ESTABLISHMENT FOR THE SECURITY OF THE DISTRIBUTED COMPUTER SYSTEMS

Summary. There is suggested a method for the trust level establishment to the nodes of distributed computer systems (DCS) taken into account the dynamics of the information value changing and with the in-time records of the security incidents from the nodes. The proposed method of the DCS nodes rating establishment allows adaptively and during the DCS functioning to determine a safety configuration of resources (nodes) for the information processing in the DCS. Also, there is described the specifics of the implementation of the mechanisms for the nodes trust level establishment.

MECHANIZM OCENY W CELU USTANOWIENIA ZAUFANYCH RELACJI DLA ROZPROSZONYCH SYSTEMÓW KOMPUTEROWYCH

Streszczenie. W artykule przedstawiono metodę określenia poziomu zaufania w przypadku węzłów w rozproszonych systemach komputerowych. Bierze się w niej pod uwagę dynamikę informacji, w celu zapewnienia bezpieczeństwa węzłów. Proponowana metoda oceny węzłów pozwala określić konfigurację zasobów bezpieczeństwa dla przetważania informacji w rozproszonych systemach komputerowych. Ponadto, opisano specyfikę wdrażania mechanizmów ustanowienia węzłów dla poziomu zaufania.

1. Introduction

The information security mechanisms for the distributed computer systems should solve the following three main problems [1]:

• the integration of the developed security mechanisms into the existing computer systems;

• the interoperability of the security mechanisms with the different software platforms and environments (J2EE,. NET, Linux-server etc.);

• the trusted relationship establishment between the interacting DCS nodes.

In view of the fact, that the DCS security mechanisms cover many domains in the system, the trust relationships between them play the special role. The trust between the DCS domains and nodes may be conjectural, be based on the topological features, either be explicit, specified with the formal policies and support the mandates exchange. The trust establishment is performing separately for each session, or dynamically on demand [2]. Due to the fact that in the DCS domains there are used the different technologies (computer network authentication protocol Kerberos, public-key infrastructure – PKI etc.) during the trust establishment mechanisms implementation should be taken into consideration the specifics of the security mechanisms.

The problem of trusted relationship establishment is actual due to the need to support the dynamic and controlled launching of services, that are initiates to perform the certain tasks [2]. For example, in a distributed data processing system the temporary services are creating for data retrieving from a remote repository, as well as for the synthesis of results.

The process of the trusted relationships establishment is based on the following aspects [3,4]:

• authorization: it is required to determine exactly which subject is the initiator of service launching;

• policies establishment: subjects should be able to create their own policies, in particular, to determine the subjects, that can get access to the services and the corresponding allowable actions, and the subject's local policy must comply with the DCS security policy;

• the level of node reliability: before the tasks initiation the subject may request evaluation of the nodes reliability, which includes the following criteria: the anti-virus protection, the the firewalls implementation, the Virtual Privat Network (VPN) mode for data exchange within the DCS etc. To perform this evaluation the accreditation mechanism is commonly used, where the level of node reliability is determined on the basis of the independed experts review;

• complex formation of the policies: security policies for DCS services are created dynamically taken into consideration the several factors: the owner of the resource, the initiator of the service launch, the specifics of the virtual system, which is realized the services etc;

• access rights delegation: in some cases, the temporary services perform the actions on behalf of the subject that has created them, for example, some computational process may requests data in the different DCS domains. In this case, between the domains, which run the services and the one that the request performs, can not be established directly the trusted relationships, then the service must be able to perform actions with the rights of its subject-initiator. This requirement, in turn, raises a number of issues, including: the principle of providing the partial access rights of the subject to the service, a mechanism for resolving situations when the validity of delegated access rights will be over before the service will be complete its actions [5].

One of the possible approach to solve this problem is to implement the controlled access to DCS resources and services. The Global Grid Forum (GGF), currently named Open Grid Forum (OGF), has developed Open Grid Standards Architecture (OGSA) for the Grid systems, and the most important element of the standard is Grid Security Infrastructure (GSI), which describes the main challenges and requirements for safety ensuring for the Grid systems.

2. The mechanism for the trust level establishment between the DCS nodes

To improve the security of the distributed computer systems there is proposed the mechanism for the resources protection on the basis of the trust level to DCS nodes with the dynamic changing of the information value.

The suggested approach is the follow. During the DCS scaling each new node or domain are initially assigned with the initial minimal (possibly zero) trust level, because the behavior of this new added node in the DCS is not defined due to the absence of the any relevant statistical information.

Thus, a new added node in the initial period of its operation in the DCS structure has not sufficient trust level to operate with the confidential information and, hence, it will receive the open data only. When the node is functioned in DCS structure, the parameters of its operation and the data transmitted from this node to the DCS are monitored continuously. The need for continuos monitoring of the transmitted data from the nodes, is in particular due to the possibile situation, when a node with a low trust level is acting as an agent of the intrusions, and, for example, performs the unathorized access to DCS resources [5].

By default, the new added node is automatically accept the pre-installed security policy in the system. In the general, it is assumed that the new node trusts, at least , a node or domain of the safety administrator, supporting the basic security functions of DCS. Further, during the node is functioned in DCS structure the trust level to it is dynamically changed, and there is forming index of the node rating based on relevant statistical information.

To form the nodes ratings (the trust level) there are used the mechanisms for nodes parameters monitoring, as well as statistical data, received from the nodes with high level of trust, that are previously integrated into the system (Fig. 1) [2,5].

We suggest an approach to form the trust level of the DCS nodes on the basis of the analysis of the dynamics of the processed information value changing. Let us descibe it below.

Taken into account the processed infomation value, the trust level $Tn_i(t)$ to the i-th node is:

$$Tn_i(t) = Tn_0 * e^{\left(C(t)*\lg\left(\frac{N_{\lim}}{N_i(t)+1} \right) \right)}, \quad (1)$$

where: Tn_0 – initial trust level to the node; $C(t)$ – the function of the information value parameter for the time interval $(0, t)$, $N_i(t)$ – the number of safety incidents initiated by or

associated with the *i*-th node on a time interval *(0 , t)*, N_{lim} – the critical number of the incidents at the same time interval.

The parameter of the information value is presented as the discrete levels, for example, from 1 to 5, depending on the current requirements for the information safety, and is changing dynamically.

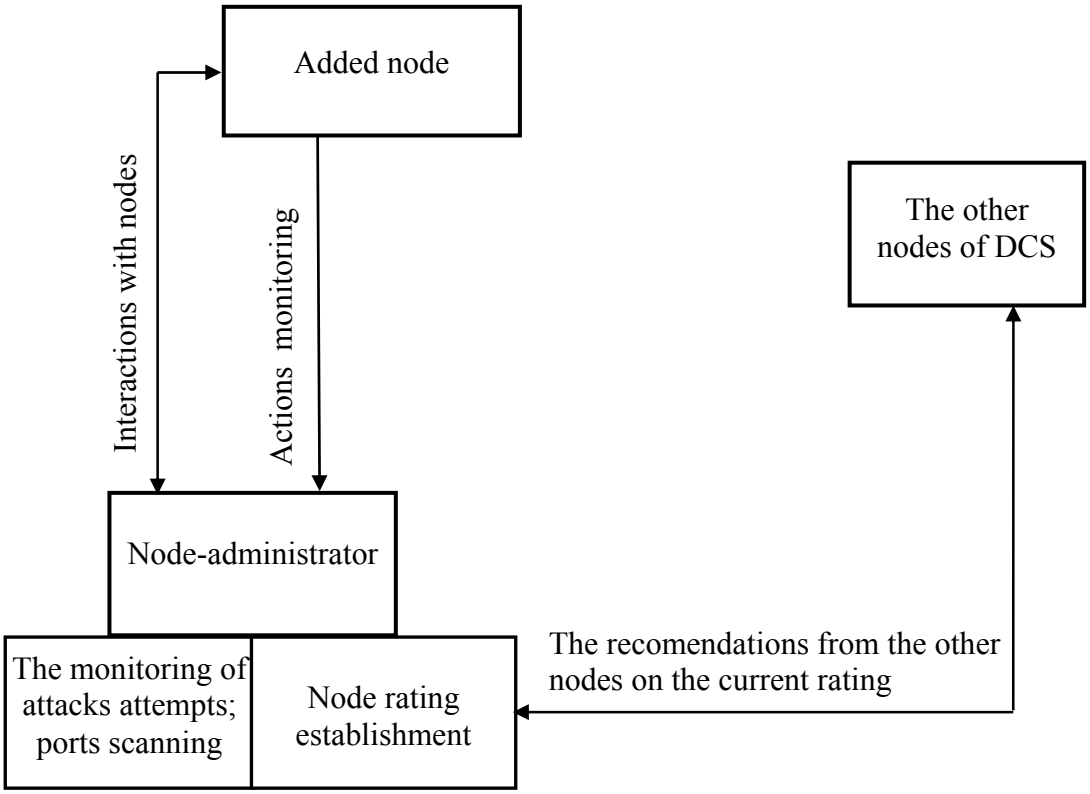

Fig. 1. The mechanism for the establishment of the DCS nodes ratings (the trust level)
Rys. 1. Mechanizm określania oceny węzłów DCS (poziom zaufania)

Security incidents in the DCS are divided into intentional and unintentional actions of the subjects. In general, the DCS subjects, and accordingly, the nodes from which they interact with DCS, can occasionally make unintentional mistakes, that are formally associated with the attempt to get unauthorized access. So, the changing of the parameter N_{lim}, which in fact, defines the maximum allowable number of security incidents caused by accidental actions of the subjects, allows to settled down this problem .

In general, the trust level Tn_i to the *i*-th node during its functioning in DCS structure can be increased, reduced or remain constant. Thus, if the number of security incidents $N_i(t)$, associated with the *i*-th node on the interval *(0, t)* exceeds the critical parameter N_{lim} $(N_i(t) > N_{lim})$, then the trust level to the node is decreased, in the other case $(N_i(t) < N_{lim})$, the trust level to the node, on the contrary, is increased.

We propose to normalize the node rating on the interval (0, ... , 1). To do this, we define the maximum possible turst level Tn_{max} to nodes in a certain DCS with a fixed initial trust level:

$$Tn_{\max}(t) = Tn_{0\,fix} * e^{\left(C_{\max} * \lg\left(N_{\lim}\right)\right)}, \qquad (2)$$

where Tn_{0fix} – the initial trust level to the node, C_{max} – the maximum level of the information value on the time interval *(0, t).*

Further, to norm the trust level the parameter Tn_i is divided by $Tn_{max.}$

The period when the node is functioned in DCS structure *(0, t)* we present as the finite observation intervals (t_k, t_l), and, depending on the results of the node behaviour in these intervals the trust level to it is reduced or increased. As a result, the changing of the trust level Tn_i to the *i*-th node is a piece-wise function.

Fig. 2 shows the possible variants of the normalized nodes ratings during its functioned in DCS structure with the dynamically changed index of the information value on the observation intervals.

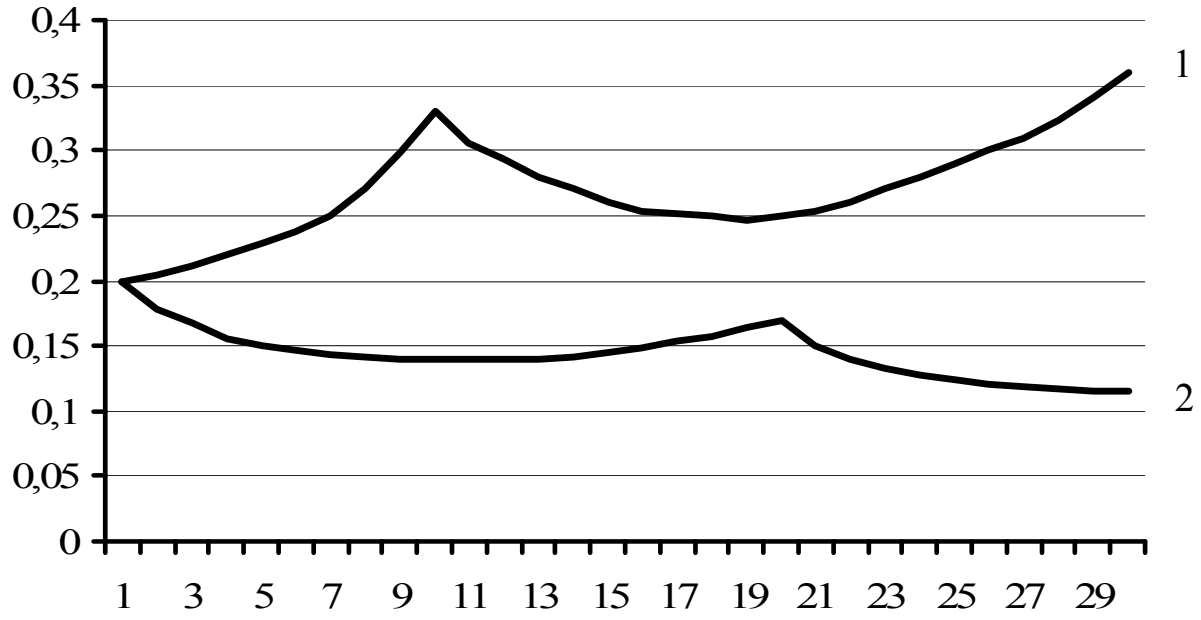

Fig. 2. The DCS nodes rating with the dynamically changed index of the information value
Rys. 2. Ocena węzłów DCS a dynamicznie zmienny wskaźnik wartości informacji

In the first case (the dependance 1) on the first interval the trust level to the node is increasing, on the second – is decreasing and on the third interval is increasing again, that is determined by two factors:

• the number of security incidents associated with the node (respectively, on the first and third interval the number of incidents is less than the critical level, on the second is above of it)

• the dynamics of the processed information value.

With the increasing of the trust level also there is increased the degree of the information value, which can be sent to this node for processing, that, in turn, in accordance with (1), further increases the trust level to the node. In the case if the node is initiated the security incidents, the trust level to it is reduced and therefore this node will receive the information with a lower value, down to the open information only. In general, the dependence 1 shows the general trend of the DCS node rating increasing, thus it should be noted that the node rating is changed gradually (continuously), but not as the jump at the end of the observation interval.

The dependence 2 is described the second case, when due to a large number of security incidents from the node the trust level to it is reduced, however, as in the previous case, on the certain observation intervals there is some local increasing of the trust level.

Figure 3 shows the variants of nodes rating changing in case, when the number of security incidents on the corresponded observation intervals (t_k, t_l) is the same as in the first and second cases discussed above, but the index of the processed information value is constant. In fact, this situation is typical when the differentiation of information by its value is not performed.

As it shows Fig. 3, in this case the main trend of the DCS node trust level changing remains the same as in the case of dynamic changes of the information value, but the index of the trust level is varying discretely (discontinuously) at the end of the observation interval, so, it does not provide the in-time adaptation to current safety requirements to DCS.

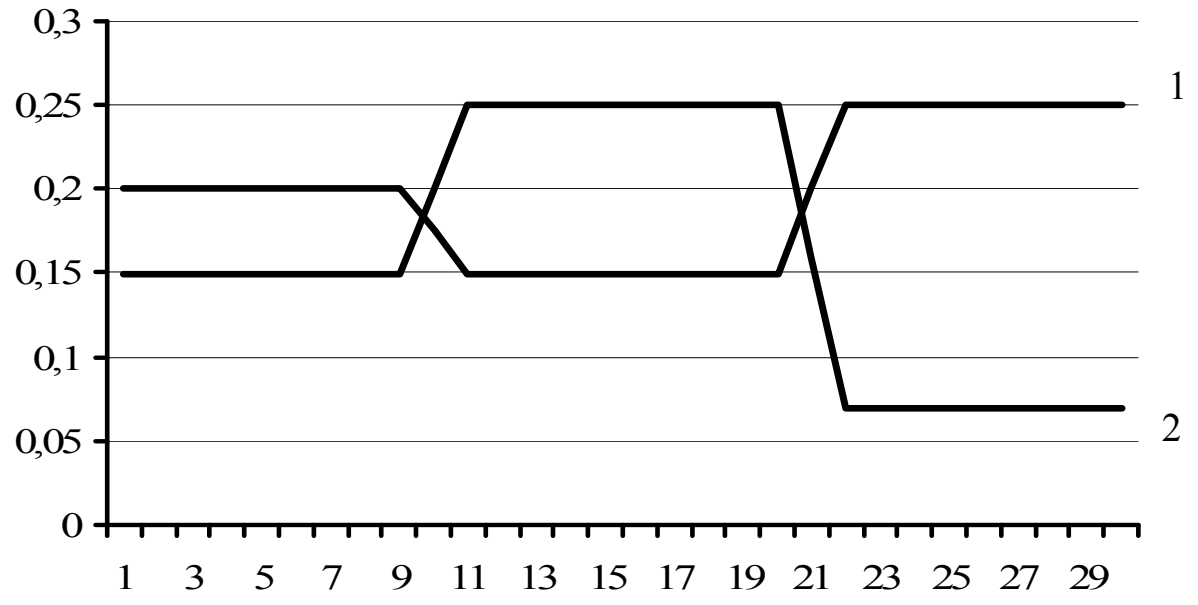

Fig. 3. The rating of DCS nodes with the constant index of the information value
Rys. 3. Ocena węzłów DCS a stały wskaźnik warości informacji

It should be noted, that in general the DCS combines a big number of nodes and, as a consequence, the centralized forming of the trust level to the each nodes in the system is rather time-consuming task, requiring the considerable time. The trust management

architecture used in the XenoServer Open Platform - XenoTrust system solves this problem by limiting the number of nodes, which send the information to change the trust level. However, in this case it is necessary to define the correct criteria for the nodes selection, which will be send information on the trust level, and to perform continuous monitoring of the received data from this node, because if the node trust level is low, the data are used to modify the trust level can be unreliable.

To solve this problem, we propose the next approach. In general, the DCS structure contains the several domains within which the nodes are located in a limited area, and are related to the the united organizational structure, so they are forming the mutual trust level based on the functioning within its local domain.

To improve the correctness of the trust level establishment procedure and to reduce the needed time for it there is sugessted to perform the average rating assessment, taking into account the mutual trust level between the nodes within the local domain. To implement this approach we propose to introduce the server with trust metrics, which, depending on the current trust level to the DCS nodes, generates the complex assessment of the nodes trust level. So, the complex trust level $Tncx_i$ to the DCS node is:

$$Tncx_i = \frac{Tns_i + \sum_{j=1}^{n} Tn_{ji} * Tns_i}{n+1}, \tag{3}$$

Where: Tns_i – the trust level to the i-th node on the server with trust metrics, Tn_{ji} – trust level of the j- th node to the i-th node (mutual trust), n – the number of nodes in the system.

Initially, the trust level for the i-th node on the server with trust metrics is set to an initial value Tns_{0i}, although, if necessary, for the certain nodes there the different from the initial Tns_{0i} trust level can be set. Further, according to the results of the node functioning in the DCS structure as part of its domain, with (1) we receive the trust levels Tns_i and Tn_{ji}, and then we form the complex trust level $Tncx_i$.

To correct the trust level in a new added node with the initial trust level Tn_{curr0} we proposed to launch the so-called test parcels, i.e. to generate data that imitatite the information with a high index values, then transfer it to the node, and to analyse the node reaction to it. In case if the node will perform the unauthorized actions to these data, the trust level to it will be decreased. Such adjustments are particularly relevant in those cases, when all the DCS nodes are processed of the confidential information and there is the critical trust level, which can not be reduced during the information processing.

3. The method for the DCS nodes rating establishment considering the dynamics of the information value changing

Let us formulate the suggested method for the DCS nodes rating establishment considering the dynamics of the information value changing.

1. To perform the ranking of information by its value, then to form a functional dependence of the information value *C(t)* in time. To each information unit (data, tasks etc.) is assigned the appropriate level of its value.
2. To calculate with (1) the trust level to the nodes from the server with trust metrics (Tns_i) and the mutual trust level between the nodes within the local domain (Tn_{ji}).
3. To calculate the current rating $Tncx_i$ of the DCS nodes with (3).
4. To correct the trust level to the new added nodes with the special test mechanism.
5. To perform the test of the possibility to send the information to the certain node before launch any transactions by comparing the current complex trust level $Tncx_i$ to this node and the required critical trust level Tn_{min}, that is defined by the safety administrator. The transaction is permitted in the case only if the current trust level to the node is greater than or equal to the required trust level ($Tncx_i \geqslant Tn_{min}$).

The suggested method for the DCS nodes rating establishment allows adaptively and during the system functioning to determine the most secured configuration of resources (nodes) for the information processing taking into account the dynamics of the information value changing, so the method allows to improve the effectiveness of the security systems in DCS. The implementation of security mechanisms, based on the proposed method allows to reach the sufficient level of security for the system, even in case when the new node is added during the scaling of the distributed system, what is especially important in the real practice.

4. The implementation of the security mechanisms for the DCS based on the trust level establishment

In accordance with the recommendations of the OGF, the security mechanims are implemented in the DCS as the additional tools to the already existing hardware and software mechanisms which support the distributed computing [6,7]. To implement the proposed method for the DCS nodes rating establishment we suggest the special structure of the safety mechanism, which includes the tools for the evaluation and analysis of the trust level to the nodes (Fig. 4). This structure is consistent with the basic requirements of OGF to the DCS security mechanisms: there are present the mechanisms for the network security, authorization and authentication, for the security of the transmitted messages, and it may be expanded to include additional mechanisms [1,6,7].

All the security mechanisms form an united system, but each mechanism is independent from the others. The one of the most important components is the security monitoring service, which also takes part in the formation of the trust level to the nodes. This service includes the tracking subsystem, affecting on the nodes trust level. Also, this service performs the monitoring of the all critical events in the DCS. In particular, it monitors the processes of the identification, authentication and the access authorization to the DCS resources [6].

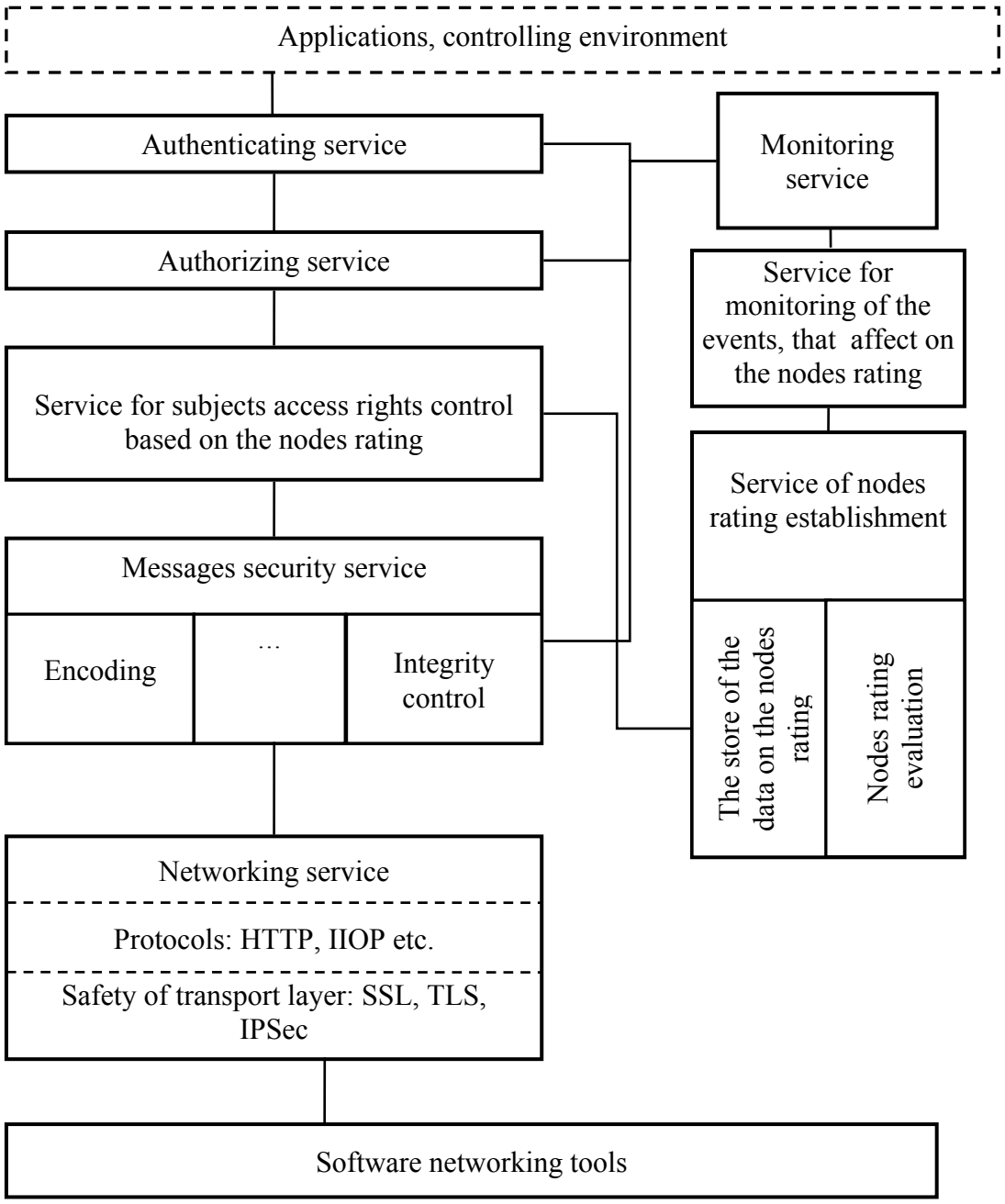

Fig. 4. Structure of the security mechanisms for DCS based on the nodes rating establishment
Rys. 4. Struktura mechanizmów bezpieczeństwa DCS na podstawie określenia oceny wezłów

The generated values of the nodes rating are transmitted to the service of the subjects access control, based on the trust level, that allows to establish a secure configuration of resources (nodes) for the information processing in DCS taking into account the dynamics of the information value changing. Also, the proposed structure includes several standard services that support the distributed computing environment, in particular, the protocol for data protection.

5. Conclusion

We suggest a method of the trust level establishment to the DCS nodes taken into account the dynamics of the information value changing and with the in-time records of the security incidents from the nodes. It is shown that the proposed method of the DCS nodes rating establishment allows adaptively and during the DCS functioning to determine a safety configuration of resources (nodes) for the information processing in the DCS, that improve the effectiveness of the security system. The implementation of the suggested method allows to support the required security level system for the DCS in case of the new nodes adding during the scaling of the distributed system.

Also, there is described the specifics of the implementation of the mechanisms for the nodes trust level establishment. It is shown that the suggested mechanisms are compliane with the main requirements for the security system for the DCS, and are expandable to include additional mechanisms.

Bibliography

1. Nagaratnam N., Janson P., Dayka J., Nadalin A., Siebenlist F., Welch V., Foster I., Tuecke S.: The Security Architecture for Open Grid Services. Publisher: Global Grid Forum, http://www.scribd.com/doc/45082834/The-Security-Architecture-for-Open-Grid-Services, p. 31.
2. Josang A., Ismail R., Boyd C.: A Survey of Trust and Reputation Systems for Online Service Provision // Decision Support Systems, 43(2), 2007, p. 618-644.
3. Luke T.W.T., Jennings N.R., Rogers, Luck M.: A Hierarchical Bayesian Trust Model based on Reputation and Group Behaviour // 6th European Workshop on Multi-Agent Systems, 18th-19th December, 2008, Bath UK.
4. Arenas A.E., Aziz B., Silaghi G.C.: Reputation Management in Grid-Based Virtual Organisations // Proc. International Conference on Security and Cryptography (SECRYPT 2008), Porto, Portugal, 26-29 Jul 2008, INSTICC.

5. Kerschbaum F. et a.l: A trust-based reputation service for virtual organization formation. In Proceedings of the 4th International Conference on Trust Management, Vol. 3986 of Lecture Notes in Computer Science, Springer 2006, p. 193-205
6. Chakrabarti A.: Grid Computing Security. // International Workshop „Advanced Computing and Communications (ADCOM)", Ahmedabad, INDIA, December 2004, p. 12.
7. Teo Y.M., Wang X.B.: ALiCE: A Scalable Runtime Infrastructure for High Performan-ce Grid Computing. // Proceedings of IFIP International Conference on Network and Parallel Computing, Springer Verlag, Wuhan, China, October 18-20, 2004, p. 101-109.

Omówienie

W artykule zaproponowano metodę ustalenia poziomu zaufania w zakresie węzłów DCS uwzględniającą dynamikę zmiany wartości informacji i dokumentacji w czasie incydentów bezpieczeństwa, dotyczącą węzłów. Wykazano, że zaproponowana metoda oceny DCS pozwala określić konfigurację bezpieczeństwa zasobów (węzłów) w celu przetwarzania informacji w DCS, aby poprawić skuteczność systemu bezpieczeństwa.

Wdrożenie proponowanej metody pozwala na poprawę wymaganego poziomu zabezpieczeń dla systemu DCS, w przypadku dodawania nowych węzłów podczas skalowania w systemie rozproszonym. Ponadto, w artykule opisano specyfikę wdrażania mechanizmów ustanowienia węzłów dla poziomu zaufania. Wykazano, że mechanizmy są komplementarne do głównych wymogów dla systemu ubezpieczeń, dla DCS i są rozszerzalne o dodatkowe mechanizmy.