Resource management in client-server computing systems based on trust assessment

R V Lebedev, A V Murigin and V S Tynchenko
Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation

E-mail: lebedev.rv@gmail.com, avm514@mail.ru, vadimond@mail.ru

Abstract. The article describes a trust assessment model and a method based on it for managing client access to scarce resources in a client-server computing system. Trust in a client is the degree to which it meets the standard. The trust assessment score is based on an ordinal preference scale with a limited normalized weight of criteria. The model allows you to get a numerical assessment of the client's compliance with a given set of criteria. The method of managing computer system resources is based on a controlled impact on the communication channel between the client and the server of the system. This method describes how to select a threshold value for the trust assessment score. The method allows you to reasonably limit the total number of clients in the system and thereby increase the probability of access to scarce computing resources of the server for trusted clients.

1. Introduction
The client-server architecture is the foundation for most corporate information systems. It is important to note that in actually functioning systems, information processing is partially retained on the client side. This is due to the peculiarities of the technological process of its processing, historical or regulatory factors. In this sense, client-server systems are similar to distributed systems, where information is processed and stored at nodes remote from each other. The system owner usually has little influence over client nodes and cannot guarantee that they will meet all quality or safety requirements.

The issues of access control in modern client-server systems, the formalization of the problem and tasks are described in [1, 2]. In modern information systems, management methods based on attributes or context (ABAC, CBAC) are widely used [3]. These approaches are implemented in many international standards such as IEEE 802.1p/q/v/x etc. Their common drawback is the strict determinism of control rules. In practice, the owner of the system often relies on some summary, aggregate information about the client, deciding whether to allow his access to the server resource. The paradigm of trust as a criterion for deciding in a control problem is actively developing [4 - 6], research is underway on various approaches to assessing the level of trust in subjects, presented in the works of researchers around the world [1, 7 - 11].

In this paper, a model for assessing trust based on comparing the access subject (client) with a standard is considered. Trust is understood as a numerical assessment of the degree of compliance of a client with a set of criteria set by the system owner.
2. Trust criteria

Trust criteria must meet the following principles:

- Objectivity - the value of the criterion should be interpreted unambiguously, it cannot depend on other factors.
- Documentation - the information being checked must be recorded in a form suitable for processing.
- Universality - the criteria of trust should be equally applicable for all clients.

Trust criteria can include information about the software and hardware composition of the client's host, the roles assigned to it, attributes, statistics of activity and incidents. Let \( M = \{ m_i \in M \mid i = 1, n, n \in \mathbb{N} \} \) denote the set of criteria for trusting the access client \( X \) in the computer system \( S \). For each \( m_i \in M \), we perform a loose ranking procedure according to the degree of importance of the criterion or its influence on the general level of similarity \( X \) with the reference. The procedure is carried out by a convenient method, for example, a sorting method: the criteria are sorted out in order and for each next \( m_i \) a decision is made: \( m_i < m_{i+1} \) is more important than \( m_i \) or \( m_{i+1} \sim m_i \) - criteria are equivalent.

Thus, on the set \( M \), a partial ordering relation will be defined such that \( \forall m_i, m_j \in M : i < j \Rightarrow m_i < m_j \vee m_i \sim m_j \). This relation will divide \( M \) into pairwise disjoint classes of equivalent criteria \( (M/\sim) = \bigcup_{m \in S} [m_j] \). We will denote by \( [m_j] \) the equivalence class of the \( m_j \) criterion, that is, \( [m_j] = \{ m \in M \mid m \sim m_j \} \). Let us introduce the recalculation function \( \varphi \) on them according to the rules (1).

\[
\varphi: (M/\sim) \to \mathbb{N},
\varphi([m_i]) = \begin{cases}
1, & \text{if } m_i < m_j \\
0, & \text{if } m_i = m_j \\
\varphi([m_j]), & \text{if } m_i > m_j
\end{cases}
\]

\[\exists i_{\text{min}} = 1, n \forall j \neq i_{\text{min}} : m_{i_{\text{min}}} < m_j \Rightarrow \varphi([m_{i_{\text{min}}})] = 1, \tag{1}\]

\[\exists i_{\text{max}} = 1, n \forall j \neq i_{\text{max}} : m_j < m_{i_{\text{max}}} \Rightarrow \varphi([m_{i_{\text{max}}})] = N.\]

We will call the rank of the trust criterion \( m \) from \( M \) the value \( R(m) = \varphi([m]) \) and the base of the scale the value \( N^M = \sum_{i=1}^{n} R(m_i) \). The rank of the trust criterion is defined as the value of the recalculation function for the equivalence class \( m \), and the base of the scale - as the sum of the ranks of all trust criteria in \( M \). We introduce the concept of the criterion weight \( W(m) \) as the ratio of the criterion rank to the base of the scale (2).

\[
W(m) = \frac{R(m)}{N^M} = \frac{\varphi([m])}{\sum_{k=1}^{n} \varphi([m_k])}, \tag{2}
\]

In this case, the properties (3) are valid for the value \( W(m) \): the total weight of all trust criteria in \( M \) is equal to 1; higher-ranked trust criteria carry more weight.

\[
W(M) = \sum_{i=1}^{n} W(m_i) = 1,
\forall m_i < m_j \Rightarrow W(m_i) < W(m_j). \tag{3}
\]

Based on the introduced concepts, let's move on to the description of the assessment of trust in client \( X \) in the system. Let client \( X \) be given by a tuple of binary values \( (x_1, \ldots, x_n) \) that determine the fact that the client meets the trust criteria from \( M \). The function \( T(X): M \to [0; 1] \) is called the client's trust score (4).

\[
T(X) = 1 - \sum_{i=1}^{n} x_i \cdot W(m_i) = 1 - \frac{1}{N^M} \sum_{i=1}^{n} x_i R(m_i). \tag{4}
\]

The trust assessment function (4) is the basis of the method for controlling access of clients \( X \) to the server of system \( S \).
For any client $X$, we denote by $X^t$ the state of $X$ at time $t$. Similarly, if $x_i$ is the value of the $i$th trust criterion for client $X$, then $x^t_i$ is the value of the $i$th trust criterion for client $X$ at time $t$. Also, if $T = T(X)$ is the value of the trust score for client $X$, then $T^t = T(X^t)$ is the value of the trust score for $X$ at time $t$.

We will call the step of increment of the trust score $\Delta T$ the value by which the value of the trust score function $T(X)$ changes when the value of one trust criterion for the client $X$ changes:

$$\Delta T = T(X^1) - T(X^0) = \frac{R(m_i)}{N^M},$$

$$\exists i \in [1, n]: X^0 = (x_1, ..., x_i, ..., x_n), X^1 = (x_1, ..., \neg x_i, ..., x_n). \quad (5)$$

We will denote by $\epsilon$ the value of the minimum increment step and $E$ the value of the maximum increment step of the trust estimate $\Delta T$. It follows from condition (1) and formula (5) that the value of $\Delta T$ is determined by the rank of the variable value of the trust criterion $m_i$ from $M$. Therefore, the specified conditions for $\epsilon$ and $E$ will be fulfilled for the values of $R(m_i)$ equal to 1 and $N$, respectively:

$$\epsilon = \min(\Delta T) = \frac{1}{N^M}$$

$$E = \max(\Delta T) = \frac{N}{N^M}. \quad (6)$$

Let us call the trust threshold $Z$ the minimum value of the trust assessment function $T(X)$ to the client $X$, at which he will be considered trusted in the system $S$. In a formal form, this condition can be written as (7):

$$T(X) > Z \Rightarrow X \xrightarrow{\text{access}} S. \quad (7)$$

Within the framework of this model, it is important to determine the approach to choosing the value of the trust threshold $Z$. Based on the previously described order of ranking of the trust criteria, it will be logical to rely on the most significant trust criteria from $M$, their weight and, as a consequence, the degree of influence on the value of the estimate $T(X)$. From these considerations, for the problem of controlling client access, we will consider two boundary options for determining the threshold $Z$.

With the most loyal approach, in order to lose trust in himself, client $X$ should not meet the criteria, with a total weight equal to all criteria from the class of the most significant criteria $[m_n]$:

$$Z = 1 - [[m_n]] \cdot E. \quad (8)$$

The most demanding approach assumes loss of trust if the total weight of $X$ criteria not met by the client reaches the weight of at least one criterion from $[m_n]$:

$$Z = 1 - E. \quad (9)$$

It is important to note that the choice of the threshold $Z$ does not make sense to determine in absolute terms, since with a possible change in the structure of the set of trust criteria and recalculation of their weights, the trust threshold should also be adjusted.

3. Access control

The access control method from the point of view of the classic client-server architecture assumes a controlled impact on the communication channel between the client and the server. The general scheme of the control system is shown in figure 1.

For clients with a level of trust below the set threshold, the communication channel is blocked, and the server does not receive an authorization request from the client, thus untrusted clients cannot connect to the system.

The effectiveness of the proposed method can be substantiated through the apparatus of multichannel queuing systems of a closed type with zero queue and refusals [12 - 16].
It is considered that the system $S$ has a limited computing resource for servicing clients $X$ and allows simultaneous connection of no more than $\omega$ clients. In turn, $X$ consists of a limited and known number of terminal nodes $\chi$, each of which creates the simplest flow of requests for access to $S$ of intensity $\lambda$ and releases a busy channel with intensity $\mu$. We assume that $\chi \geq \omega$, and in the case when all $\omega$ channels are busy, all incoming requests for access are refused and immediately returned back to the source. The system state graph is shown in Figure 2.

The calculation of the probabilities of an arbitrary state of the system $P_k$ is performed by the formula (10):

$$P_k = \frac{\chi^{|k|}}{k!} \rho^k P_0 = C_{\chi}^k \rho^k P_0,$$

where $\chi^{|k|}$ is a factorial polynomial of degree $k$, $C_{\chi}^k$ is a binomial coefficient from $\chi$ with respect to $k$.

Then, considering the total probability of the states of the system, the formula can be refined the formula for the state $P_k$:

$$\sum_{i=0}^{\omega} P_i = P_0 \sum_{i=0}^{\omega} C_{\chi}^j \rho^i = 1 \Rightarrow P_k = C_{\chi}^k \rho^k (\sum_{i=0}^{\omega} C_{\chi}^j \rho^i)^{-1}.$$

From the generalized formula (11) of the probability of the state of the system, we can express the average number of simultaneously occupied channels $\overline{\omega}$:

$$\overline{\omega} = \sum_{i=0}^{\omega} k P_k = \sum_{k=0}^{\omega} (\chi - \omega + k) P_k = \chi \sum_{k=0}^{\omega} P_k - \sum_{k=0}^{\omega} (\chi - k) P_k =$$

$$= \chi - (\chi - \omega)P_\omega - \sum_{k=0}^{\omega-1} (\chi - k) P_k = \chi - (\chi - \omega)P_\omega - \sum_{k=0}^{\omega-1} (\chi - k) C_{\chi}^k \rho^k P_0 =$$

$$= \chi - (\chi - \omega)P_\omega - \frac{\overline{\omega}}{\rho} \Rightarrow \frac{\overline{\omega}(1+\rho)}{\rho} = \chi - (\chi - \omega)P_\omega \Rightarrow$$

$$\overline{\omega} = \frac{\rho}{1+\rho} (\chi - (\chi - \omega)P_\omega).$$

The calculation of the absolute throughput $A$ of system $S$ can be performed using formulas (13):
\[
A = \lambda (\chi - \bar{\omega})P,
\]
\[
A = \lambda (\chi - \bar{\omega} - (\chi - \omega)P_\omega),
\]
(13)

where \(P\) is the probability of the system \(S\) being ready to service requests from \(X\).

From relations (13), the formula for \(P\) can be written as
\[
P = \frac{\chi - \bar{\omega} - (\chi - \omega)P_\omega}{\chi - \bar{\omega}} = 1 - \frac{\chi - \omega P_\omega}{\chi - \bar{\omega}}.
\]
(14)

The system of equations (15) composed of formulas (11), (12) and (14) fully describes the probability \(P\) of the system \(S\) to service requests from clients \(X\).

\[
\begin{cases}
P = 1 - \frac{\chi - \omega}{\chi - \bar{\omega}} P_\omega, \\
\bar{\omega} = \frac{\rho}{1+\rho} (\chi - (\chi - \omega)P_\omega), \\
P_\omega = C_X^\omega \rho^\omega (\sum_{i=0}^\omega C_X^i \rho^i)^{-1}.
\end{cases}
\]
(15)

Application of the described method of access control based on the assessment of the level of trust \(T(X)\) to clients \(X\) limits their ability to gain access to the system according to condition (7). Considering that the client is specified by a set of parameters \(X = (x_1, x_2, ..., x_n)\), independent of other clients and the state of the system \(S\), we can consider the successful result of checking trust in the client at the current time as a random event with the probability \(P_T\), determined by the trust threshold \(Z\). In this case, for the client, a refusal based on the verification of the level of trust is equivalent to a refusal of service when the system is fully loaded (in the \(S_\omega\) state).

State graph of a model of a closed-loop queuing system with failures and a zero queue for a client-server system using an access control method based on trust score is presented in figure 3.

![Figure 3. State graph of a model of a closed-loop queuing system with failures and a zero queue for a client-server system using an access control method based on trust score.](image)

By analogy with formula (10), the probability \(\bar{P}_k\) of the state of the system \(S_k\) in the mode of verification of trust in access clients can be derived from formula (16):
\[
\bar{P}_k = \frac{\chi^k}{k!} \rho^k P_0 = C_X^k \rho^k P_T P_0.
\]
(16)

Moreover, considering formula (13), the equality \(\bar{P}_k = P_k^k P_k\) is true. If we assume \(\bar{\rho} = \rho P_T\), then the general formula for the probability \(\bar{P}_k\) of the state of the system \(S_k\) from (11) and (16) will have the form:
\[
\bar{P}_k = P_T^k P_k = C_X^k \rho^k P_T^k (\sum_{i=0}^\omega C_X^i \rho^i P_T^i)^{-1} = C_X^k \rho^k (\sum_{i=0}^\omega C_X^i \rho^i)^{-1}.
\]
(17)

Considering formula (17), we can write the system of equations (15) for \(\bar{P}\) of the probability of the system \(S\) being ready to process requests for access from clients \(X\) using the access control method based on checking the level of trust in the client in the following form:
\[ \begin{aligned} \bar{p} & = 1 - \frac{x-\omega}{x-\bar{\omega}} \bar{p}, \\ \bar{\omega} & = \frac{\bar{p}}{1+\bar{p}} (x - (\chi - \omega) \bar{p}), \\ \bar{p}_\omega & = c_\omega \bar{p}^\omega (\sum_{i=0}^\omega c_i^\omega \bar{p}^i)^{-1}, \\ \bar{p} & = \rho \bar{p}_T. \end{aligned} \] (18)

It can be seen from the system of equations (15) that the probability of system \( S \) being ready to service requests for access from clients \( X \) is completely determined by their number \( \chi \), the total number of channels \( \omega \), and the load factor \( \rho = \lambda/\mu \). Considering that the computing resource of the system is determined by its software and hardware composition, we can assume that \( \omega = \text{const} \). It is also possible to consider \( \rho = \text{const} \), since the intensity of requests for access from clients and the duration of their stay in the system is determined by the specifics of the tasks solved through it. From these considerations, we can conditionally consider the probability of system availability as a function of the number of its active clients:

\[ P = P(\chi) : \mathbb{N} \to [0;1]. \] (19)

In turn, the probability \( P_T \) of passing the verification of the level of trust to the access client depends on the choice of the value of the trust threshold \( Z \). The estimate of the probability \( P_T \) can be directly related to \( Z \) based on its definition, and then we can assume:

\[ P_T = P_T(Z) : [0;1] \to [0;1], \bar{p} = P(\chi,Z) : \mathbb{N} \times [0;1] \to [0;1]. \] (20)

We will consider the efficiency indicator of the access control method \( \Delta P \) is the ratio of the difference between the estimate of the probability \( \bar{P}(\chi) \) of the readiness of the system \( S \) to service requests from clients using the developed access control method and the probability \( P(\chi) \) of the readiness of the system \( S \) to without using this method, and the value \( P(\chi) \):

\[ \Delta P = \frac{\bar{p} - P}{P}. \] (21)

4. **Experimental study and results discussion**

In practice, the calculation of the efficiency \( \Delta P \) is performed according to the initial data indicated below (table 1).

**Table 1. Initial data.**

| Parameter                        | Designation | Value | Note                                                                 |
|----------------------------------|-------------|-------|----------------------------------------------------------------------|
| Total number of clients          | \( \chi \) | 400   | Rounded number of potential customers in the system                  |
| Computing resource of the system | \( \omega \) | 100   | Computing resource of the system ensures the simultaneous operation of 25% of the total number of potential customers |
| intensity of customer calls      | \( \rho \) | 4     | Intensity of client requests to the system is 4 times greater than the intensity of the system resource release after gaining access |
| Number of trust criteria         | \( |M| \)    | 13    | Total number of trust criteria used to assess trust in access clients; each criterion is assigned a unique identifier (code) |
| Trust threshold, option 1       | \( Z_1 \)  | 0.85  | Hard variant of the threshold of trust in the access client, defined as \( 1 - E \) |
| Trust threshold, option 2       | \( Z_2 \)  | 0.7   | The soft version of the threshold of trust in the access client, defined as \( 1 - |M^N| \cdot E \) |
The result of ranking the trust criteria in terms of importance is given in Table 2, the value of the rank determines the importance of the criterion from the lowest to the highest.

**Table 2. Weights of the trust criteria.**

| Rank | Trust criterion number |
|------|------------------------|
| 1    | 1                     |
| 2    | 2                     |
| 3    | 3                     |
| 4    | 4                     |
| 5    | 5                     |
| 6    | 6                     |

Table 3 shows the calculation of the weights of the trust criteria by the above formulas.

**Table 3. Calculation of the trust criteria weights.**

| Criterion rank | Power of the group of criteria | Total weight of the group | Total normalized weight of the group | Normalized weight of the criterion |
|----------------|-------------------------------|---------------------------|-------------------------------------|-----------------------------------|
| 1              | 3                             | 3                         | 0.075                               | 0.025                             |
| 2              | 3                             | 6                         | 0.15                                | 0.05                              |
| 3              | 2                             | 6                         | 0.15                                | 0.075                             |
| 4              | 2                             | 8                         | 0.2                                 | 0.1                               |
| 5              | 1                             | 5                         | 0.125                               | 0.125                             |
| 6              | 2                             | 12                        | 0.3                                 | 0.15                              |

The normalized weight of the rank 1 criterion corresponds to the value $\varepsilon$ of the minimum increment of the trust score. Similarly, the normalized weight of the rank 6 criterion corresponds to the value $E$ of the maximum increment of the estimate. Based on these values, variants of the trust threshold values for calculations were selected.

According to the introduced trust criteria, we will assess the trust in access clients in all general population. The final distribution of ratings is shown in Figure 4.

**Figure 4. Distribution of trust ratings to clients’ access.**

Possible values of the trust score $T(X)$ are marked on the histogram along the horizontal axis, and the columns indicate the number of customers with the corresponding score value. The probability of a successful trust check by a randomly selected client can be estimated as the ratio of the number of trusted clients to the total sample size. So, for a given value of the trust threshold $Z = 0.85$, the probability of passing the test is $P_T \approx 0.67$. 
Figure 5 shows the graphs of the values $P(\chi)$ and $\tilde{P}(\chi)$ of the probability of the availability of the system $S$ with the initial parameters from table 1 in the standard mode and when using the trust estimate with a given threshold value.

![Graph of the dependence of the probability estimates $P(\chi)$ and $\tilde{P}(\chi)$ on the number of clients in the system.](image1)

**Figure 5.** Graph of the dependence of the probability estimates $P(\chi)$ and $\tilde{P}(\chi)$ on the number of clients in the system.

Figure 6 shows a graph of the dependence of the efficiency indicator $\Delta P$.

![Distribution of trust ratings to clients’ access.](image2)

**Figure 6.** Distribution of trust ratings to clients’ access.
The graph shows that for the strict version of the trust threshold $\Delta P \rightarrow 0.49$, i.e. the assessment of the likelihood of the system being ready to serve trusted clients is significantly increased.

5. Conclusion
The method presented in the framework of this study is advisable to use in conditions of a noticeable shortage of computing resources, when the owner of the system is not able to fairly divide it among all clients and is forced to choose whom to allow access in the first place.

The increased chances of trusted clients gaining access to the server are provided by denying this access to other clients. Therefore, the system owner must carefully select the trust criteria and the evaluation threshold.

References
[1] Devyanin P N 2013 Computer systems security models. Access control and information flows (Moscow: Hot line Telecom) p 338
[2] Devyanin P N 2017 On the problem of representation of the formal model of security policy for operating systems Proceedings of ISP RAS 27(3) 7-16
[3] Zeng W 2015 Content-Based Access Control: PhD thesis (USA: University of Kansas) p 152
[4] Durakovskiy A P, Kondratiev T A, Lavrukhin Yu N and Petrov V R 2020 About trust in the information systems on the basis of internet-based technologies (Moscow: MEPhI)
[5] Denning D E 1992 A New Paradigm for Trusted Systems (USA, Washington: Georgetown University)
[6] Marsh S 1994 Formalizing Trust as a Computational Concept: PhD thesis (UK: University of Stirling) p 184
[7] Beshta A A 2012 The architecture of an agent of control over an internal attacker based on a trust assessment mechanism Izvestia SFedU. Engineering 137(12) 104-10
[8] Talanov M A and Timokhovich A S 2017 Automation of assessing the level of trust in information security Academy 6(57) 8-9
[9] Arenas A, Aziz B and Silaghi G 2009 Reputation management in collaborative computing systems Security and Communication Networks 3(6) 546-64
[10] Rosaci D, Sarne G and Garruzzo S 2012 Integrating Trust Measures in Multi-Agent Systems International Journal of Intelligent Systems 27 1-15
[11] Salehi-Abari A and White T 2010 DART: Distributed Analysis of Reputation and Trust Framework (Canada: Carleton University) p 35
[12] Gilmudtirov R F and Kirpichnikov A P 2012 Mathematical model of a closed one-channel queuing system Bulletin of Kazan Technological University 6(15) 189-93
[13] Antamoshkin O A, Kilochitskaya T R, Ontuzheva G A, Stupina A A and Tynchenko V S 2018 Multicriterion problem of allocation of resources in the heterogeneous distributed information processing systems Journal of Physics: Conference Series 1015 032162
[14] Gilmudtirov R F and Kirpichnikov A P 2012 Closed multichannel queuing systems with failures Bulletin of Kazan Technological University 10(15) 232-4
[15] Gilmudtirov R F and Kirpichnikov A P 2012 Multichannel queuing systems of closed type Bulletin of Kazan Technological University 8(15) 326-31
[16] Tynchenko V S, Tynchenko V V, Bukhtoyarov V V and Agafonov E D 2018 Decision support system for designing an effective configuration of a computing network for distributed complex problem solving IEEE 2018 3rd Russian-Pacific Conference on Computer Technology and Applications pp 1-6