THE ANNALS OF "DUNĂREA DE JOS" UNIVERSITY OF GALATI
FASCICLE III, 2022, VOL. 45, NO. 1, ISSN 2344-4738, ISSN-L 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS
Article DOI: https://doi.org/10.35219/eeaci.2022.1.05

CALCULATION AND REASSESSMENT OF THE TRUST LEVEL GIVEN TO MEMBERS OF VIRTUAL ORGANIZATIONS

Laura Danilescu*, Marcel Danilescu**

* *"Dunărea de Jos" University of Galati, Faculty of Automation, Computers, Electrical Engineering and Electronics*
***ASWIC Ltd.*

Abstract: In this paper we set out to introduce new elements when calculating the level of trust given to a new member of a virtual organization. Compared to previous works, we have introduced new elements: the initial trust whose value results from sociological and psychological considerations and a reassessment of the trust by introducing feedback elements in the calculation formulas. The trust values thus calculated will be the elements on which the trust-based security policies of the organization will be built.

Keywords: trust level, feedback, situation importance, situation usefulness, knowledge.

1. INTRODUCTION

Trust is a social phenomenon and is present wherever there are societies (Yamamoto, 1990; Baier, 1986).

In previous work, we have presented the possibility of using trust as a method of enforcing security policies (controlling access and user actions) within organizations. Also, within these policies, we have presented the necessary conditions to be fulfilled, so that a user can access the data and information of the organization, taking into account that is associated with a level of trust based on direct knowledge, knowledge that also incorporates characteristics of his personality (studies, knowledge, capabilities, goodwill, loyalty, etc.).

In this paper, we will address the integration of new members within an organization that has built a mechanism for controlling access and user actions based on trust.

2. TRUST AS A DEFINING ELEMENT IN THE EXISTENCE OF ORGANIZATIONS

Trust within a group develops from cognitive, affective, behavioral and contextual perspectives. Attitudes of trust are adjusted in the time the group interacts and how the context of the group influences this development process. Attitudes of trust are feelings or dispositions held by one person towards another. Trusting behaviors are behavioral manifestations of this attitude, such as information sharing, delegation, risk-taking, and monitoring (Wildman *et al*., 2012).

In previous papers, we have addressed the issue of virtual organizations, which are types of advantageous organizations due to their flexibility and adaptability, and, which often compose highly interdependent teams of qualified people to complete complex projects.

From the point of view of the quantifiable value of the trust level given to the new member of the organization, for the position he holds, he will have a value of 0,5 (average neutral value of "distrust" = 0 and "blind trust" = 1) (Danilescu, 2022), for the actions he must take. By giving this level of trust, we are considering the results of sociological research, according to which very low trust can lead to negative consequences, such as conflict, and very high trust can lead to complacency and a reduction in the necessary monitoring behavior. (Wildman *et al.*, 2012)

At the beginning, when a new member joins a team, initial trust will be the most difficult to quantify, being based on surface-level indicators and a set of information that the new members brings with them that will influence the formation of trusting attitudes within the team. (Wildman *et al.*, 2012)

Initially, trust based on competence, benevolence and/or integrity is by definition very ambiguous, given that there is not enough prior knowledge on which to build an accurate assessment of the trust level. (Wildman *et al.*, 2012)

Imported information plays an important role in determining initial trust level. These can be defined as pre-existing knowledge, stereotypes and preconceptions stored in the memories of group members. Imported information can come from two main sources: personal experiences of team members and third-party information provided by trusted sources.

Although team members have not worked together previously, they are assumed to have worked in similar situations with similar types of people. Each new work experience will generate, for team members, a certain amount of information that will become the imported information into future experiences. (Wildman *et al.*, 2012)

Participation in the organizational life, involves collaboration not only with the members of the group in which the new member was inserted, but also participation in various activities together with the members of the other groups of the organization, projects and, implies the contribution of theoretical and practical knowledge, which the new member has stated that he would have.

Trust at the individual level is continuously adjusted following the cyclical feedback given by group members following the completion of team processes.

Team processes are defined as "the interdependent actions of members that transform inputs into outputs through activities designed to organize tasks to achieve collective goals." (Wildman et al., 2012).

A pattern of team processes was observed, based on time stages:

- the organizing stage - the team focuses on things like planning and formulating strategy;

- action stage - the team actively pursues goals and engages in task-oriented behavior;

- the post-action reflection stage – is the stage of entering the results, after the team has completed its tasks. The feedback will help to reassess the level of trust associated with the result, in the subsequent context in which the group will find itself.

- the stage of entering the results where it is useful to complete a questionnaire (Table 1).

Table 1. Questionnaire for feedback given to a group member

Feedback questionnaire completed by a recommendation agent *x* for a *y* member of the group		
$F_x(y)_1$	Communication	*y* communicates information reliably and consistently
$F_x(y)_2$	Concerned	*y* is concerned about the work-related problems of others
$F_x(y)_3$	Confidence	*y* has confidence in each other's competence to perform tasks
$F_x(y)_4$	Cooperation	*y* cooperates with colleagues
$F_x(y)_5$	Fairness	*y* treat others fairly and justly
$F_x(y)_6$	Feedback	*y* seek feedback from others when making decisions
$F_x(y)_7$	Helpful	*y* help others in need
$F_x(y)_8$	Honesty	*y* is honest in its communication
$F_x(y)_9$	Receptivity	*y* is open to feedback and help from others
$F_x(y)_{10}$	Responsibility	*y* take responsibility for its actions
....	....	....
$F_x(y)_n$	....	....

The feedback values $F_x(y)_i$ completed by the recommendation agent *x* for the *y* member of the group further constitute a basis for calculating the trust given to the *y* member of the group, at a certain time *t*, in a given situation α, which has a certain importance *I* and utility *U*.

3. BRIEF OVERVIEW OF TRUST THEORY FROM PREVIOUS PAPERS

We will resume the description of the conditions that a member of the organization, hereinafter referred to as "user", must meet in order to access and apply various processes to objects constituted in groups of objects with (1, n) members, which have the same trust value.

"We define a hierarchy as a finite set of values (H1 ≤ H2) ordered in ascending order." (Danilescu L. and Danilescu M., 2010)

"We define a sub hierarchy (I1 ≤ I2) as a subset of a hierarchy (H1 ≤ H2) if (I1 ≤ I2) □ (H1 ≤ H2)". (Danilescu L. and Danilescu M., 2010)

To these are added the following definitions: (Danilescu M. and Danilescu L., 2021):

A_k = an action k applied to an object;
C_k = the context of trust k, for accessing an object and applying an action;
C_x = the set of contexts in which the objects in the GO group can be accessed;
of_v = the delegation v, received from any user U_k;
DE = set of delegations;
Di = the domain to which GO belongs;
F_k = flow sequences k (transfer of objects from one user to another);
G_m = the group of users to which a certain user U_k belongs;
GO = object group;
$H(A)$ = partial hierarchy of actions corresponding to the subprocess p_k;
$H(E)$ = partial hierarchy of events;
O_i = Object i;
$H(p)$ = partial hierarchy of processes;
p_k = the process k applied to the object O_i by means of a user U_k;
$p_1 .. p_n$ = the set of processes of O_i;
R_u = trust level for user U_k for accessing the object O_i;
R_g = trust level for group G_m for accessing object O_i;
R_p = the trust value required to execute a process;
re_v = the restriction applied to a user;
RE = set of restrictions;
t_i = the time at which a process is applied to an object ($t_{i-1} \leq t_i \leq t_{i+1}$);
Uk = the user designated to perform an action;
Ux = any user belonging to group G_m;
V = the required trust value of the domain D_i;
$p_k(O\text{¿¿}i)^{t_i}\text{¿}$ = the p_k process applied to the object O_i at the time t_i.
The trust given to a user for the application of a certain process is expressed as follows:

(1) "For $\forall O_i \in GO \Rightarrow \exists\, p_{k(Oi)} \in H(p)$ where $H(p)=(p_1,p_2,..,p_k...p_n) \wedge \forall\, p_k = A_k \in H_k(A)$□$E_k \in H_k(E)$□$\Sigma\ F_k$,
$(\exists\, (U_k \in G_m \Rightarrow \exists\, R_u,\ R_u(U_k) \geq R_p(p_k(O_i)) \wedge R_u(U_k) = R_g) \vee \exists\, (U_x \in G_m \Rightarrow \exists\, R_u,\ R_u(U_x) \geq R_u(U_k) \wedge \exists\, de_v(U_k)$ for $U_x) \vee \exists\, (U_x \in G_m \Rightarrow \exists\, R_u,\ R_u(U_x) \geq R_u(U_k) \wedge \exists\, de_v(U_k),\ U_x \Rightarrow re_v(U_k) \in RE \wedge \neg\exists\, re_v(U_x) \in RE) \wedge \exists\, C_k \in C_x, \wedge R_g(G_m) \geq V(D_i) \Rightarrow \exists\, p_k(O\text{¿¿}i)^{t_i}\text{¿}$ "
(Danilescu M., 2022)

"For any object that belongs to a group of objects that have the same trust value, there is at least one user that belongs to a group of users who have the same level of trust, who can apply a certain process The trust given to the user is greater than or equal to the trust required to apply that process." (Danilescu M., 2022)

4. PRESENTATION, RECOGNITION, INTEGRATION AND GIVING FEEDBACK TO NEW MEMBERS OF THE ORGANIZATION. CREATING VERIFICATION AND VALIDATION POLICIES

Organizations generally have a hierarchical structure, but there may also be other structures, which we will not develop in this paper. A brief review of them was made in previous works.

Bringing a new member into the organization involves replacing another member of the organization or, adding it to the existing team.

For the selection of a new member within the organization, recommendation agents can be used

After selecting the optimal candidate, who meets the requirements of the organization, it, for a start, is assigned the basic tasks for which its competence was needed. Its introduction into the collective involves its presentation (identity, skills, studies, etc.), following that the members of the group establish the initial trust that can be granted to him. From their point of view, the new member may or may not be a known person. The person, if known, may have collaborated with the organization or not.

In any situation, the presentation of the new member of the organization, regardless of the position he occupies (manager of a compartment or field of activity, or simple member), to begin with, implies an apriority evaluation by the group members. That assessment shall be based either on pre-existing knowledge stored in the group's memory, or acquired from a third party, or on previous personal experiences, which may be used to interpret perceived cues and, consequently, to influence trust in the new member.

The initial perception cannot be changed until after a period of time, when effective participation in organizational life allows for feedback from members of the organization. The initial trust granted allows it access to internal data, information and documents that may have a certain level of internal classification. We can represent this organization in a hierarchical pyramidal form that takes into account the quantity and quality of information (Fig. 1).

From a quantitative point of view, the basic information is the most numerous; its processing takes place at the mid-level, where is created the information for the top level; at this level the information is less numerous, but it is more important.

From the point of view of the hierarchy, regardless of the form of internal organization, [thesis page 58] at the level of the working group, a hierarchical structure is implemented that overlaps the informational-decisional structure, allowing the optimization of the functionality. In this functional hierarchy, each member has its duties, responsibilities and functions well determined.

Inserting the new member into organization, assigning responsibilities, creating access to organization's data, information, and tasks, without further validation of its work, can lead to losses (Fig. 2). From this point of view, it follows the importance of the feedback of the activity of the new member within the organization.

To illustrate the above, we will consider an organization that has various fields of activity, to which is added a new member, who can be hired on a new position or can be a replacement for a former or current employee who is unavailable.

The group's feedback on the new member includes the parameters that quantify its experience, knowledge, goodwill, work capacity, loyalty, etc., depending on the profile of the organization. (Danilescu, 2022).

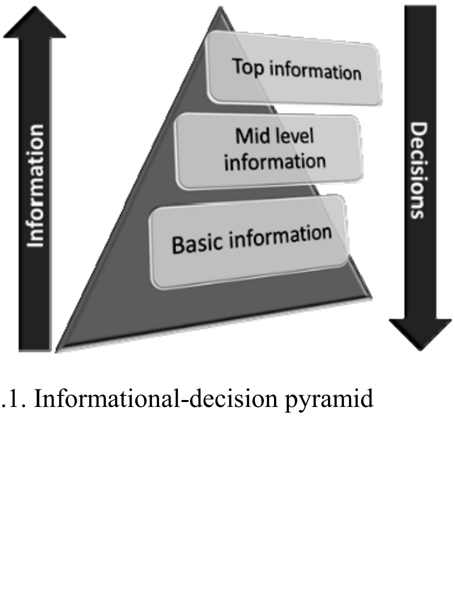

Fig.1. Informational-decision pyramid

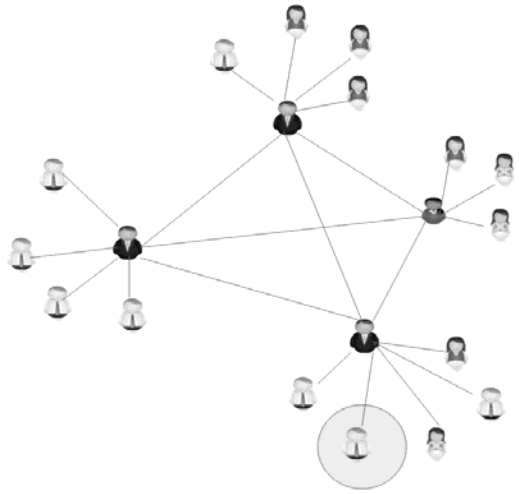

Fig. 2. A new member in the organization

This feedback may constitute a mechanism for analyzing and recommending a new position for the member of the organization and building access control policies and its actions within the informational system. In order to obtain feedback, the questionnaire method can be used that it should reflect the appreciation values given by the group members. Based on these appreciation values, the trust values can be recalculated, given that the initial trust was granted on the basis of the recommendations, without having yet to have feedback.

From (Marsh, 1992) we use the following elements :

Table 2. Items used to recalculate the trust value

Element	Meaning	Value
α,β,δ	situations	
K	knowledge	True/False
$K_x(y)$	the degree of knowledge of y by x	True/False
$K_x(y)^t$	knowledge of y by x at the time t	True/False
$I_x(\alpha)$	the importance of the situation for x	[-1,1]
$I_x(\alpha)^t$	the importance of the α situation for x at time t	[-1,1]
$U_x(\alpha)$	the usefulness of the α situation for the user x	[-1,1]
$U_x(\alpha)^t$	the usefulness of the α situation for user x at the time t	[-1,1]
T_x	the basic trust of x	[-1,1]

$T_x(y)$	x's trust in y	[-1,1]
T_x(y, a)	x's trust in y in the α situation	[-1,1]
T_x^t	the basic trust of x at the time t	[-1,1]
$T_x(y)^t$	x's trust in y at the time t	[-1,1]
T_x(y, a)^t	x's trust in y in the situation α at the time t	[-1,1]

Feedbacks are addressed to a specific moment, or periods of time. Their purpose is to collect the perception of those interviewed, about an event, a person, an interaction, a service, a provision, etc.
For the general calculation of the trust in a member y from the perspective of a recommendation agent x we will have:

(2) $T_x(y) = K_x(y) \times \frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z) \times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z))$

where

- $T_x(y,\alpha_z)$ represents the initial trust towards a certain characteristic manifested by user *y* from the perspective of the recommendation agent *x* in the situation α
- $F_x(y,\alpha_z)$ is the feedback value against a certain characteristic manifested by the user *y* from the perspective of the recommendation agent *x* in the situation α
- U_x, I_x, K_x , T_x may refer to a moment t or a longer duration of time

If the analysis of the situation α is carried out on quanta of time then the formula will be:

(3) $T_x(y)^t = K_x(y) \times\frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z)^t \times I_x(\alpha_z)^t \times \frac{1}{2}(T_x(y, \alpha_z)^t+ F_x(y, \alpha_z)^t))$

where t = (1..m)

(4) $T_x(y) = K_x(y) \times \frac{1}{m}\sum_{t=1}^{m} \text{¿¿}(U_x(\alpha_z) \times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z)))^t$

In order to make a feedback survey on the work of the new member of the organization, it is necessary that all participants in the investigated activity fill in the created questionnaires.

For a more balanced calculation, we will take out of the results the most unfavorable value as well as the most favorable to the y member of the organization.
The calculation of the level of trust that can be given to it becomes:

(5) $T(y)=\frac{1}{v}\text{¿}K_x(y) \times \frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z) \times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z))) - Max(K_x(y) \times \frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z) \times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z)) - Min(K_x(y) \times \frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z)\times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z)))$

for x >=5
Otherwise,

(6) $T(y)=\frac{1}{v}\text{¿}K_x(y) \times \frac{1}{n}\square_{z=1}^{n}(U_x(\alpha_z)\times I_x(\alpha_z) \times \frac{1}{2}(T_x(y, \alpha_z)+ F_x(y, \alpha_z))))$

The calculation of the general trust granted by the activity partners on the basis of the equations presented above in 5 and 6, allows the correction of the initial trust value granted to the y member of the organization.

5. CONCLUSIONS

New members who enters an organization where access control policies and trust-based actions are practiced, will receive an initial trust that will allow them access to information and execute actions according to their role in the organization. Thereafter, the trust level will be recalculated and adjusted.

Changing the initial trust values will result in the assignment of modified rights to access various objects and groups of objects in the organization through various processes that it can apply to them, according to the condition of controlling the access and actions of the users in (1). These conditions imply that the objects and groups of objects within the information system are organized hierarchically, the hierarchy being determined by their importance and the degree of sensitivity. The higher the level of trust in the designated user, the higher its importance, culminating in the CEO of the organization that has the 100% trust level.

In order to apply the calculated trust levels and determine the access rights of the members of the organization and establish the actions they have the right to take, the objects and groups of objects belonging to the fields of activity of the organization must be established.

Within each field of activity, a hierarchy of objects is established which are assigned a minimum trust value, necessary for accessing them. After establishing these hierarchies, the processes that will be applied to the objects and groups of objects above are established. They will also be organized into process hierarchies, which will also have a reliable value that will illustrate their hierarchy. The trust value in a member of the organization, previously calculated, must match or be greater than the value of the process applied to the object group. (Danilescu M., 2022).

6. REFERENCES

Yutaka Yamamoto, (1990). A morality based on trust: some reflections on Japanese morality. In: *Philosophy east and west*, **Vol. 40, No. 4**, pp. 451-469. Publisher, University of Hawai'i Press, https://www.jstor.org/stable/1399351

Baier, A. (1986). Trust and Antitrust. In: *Ethics* **Vol. 96, No. 2**, pp. 231-260. Publisher: The University of Chicago Press. https://doi.org/10.1086/292745 https://www.jstor.org/stable/2381376

Wildman, J. *et al.,* (2012). Trust Development in Swift Starting Action Teams: A Multilevel Framework. In: *DigitalCommons@University of Nebraska – Lincoln, US Army Research, U.S. Department of Defense*. https://digitalcommons .unl.edu/ usarmyresearch/162

Danilescu M., (2022). Control of access and actions in informational systems. pp.52. Publisher: National Council on Accreditation and Attestation, Chisinau, Rep.Moldova, http://www.cnaa.md /thesis/57796/.

Marsh, P.S., (1994). Formalising Trust as a Computational Concept, pp 59. Publisher: Department of Computing Science and Mathematics, University of Stirling http://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf .

Danilescu L., Danilescu M., (2010). Control Access To Information By Applying Policies Based On Trust Hierarchies. In: *International Conference on Computer and Software Modeling, ICCSM 2010*, pp. 285-290. Publisher, IEEE. https://www.researchgate.net/publication/343635735_control_access_to_information_by_applying_policies_based_on_trust_hierarchies.

Danilescu M., Danilescu L., (2021) Design of software applications using access and actions control policies based on trust. In: *2021 International Conference on Computational Science and Computational Intelligence (CSCI),* pp. 1964-1968. Publisher, IEEE. https://ieeexplore.ieee.org/ document/9798978.