Data security management applying trust policies for small organizations, ad hoc organizations and virtual organizations

Marcel DANILESCU[1]

Abstract. Privacy and data security is one of the current requirements in organizations. In this paper, we present an implementation and management method, using trust policies based on the relative knowledge of the users, in organizations with a high dynamism. Basically, security policies are based on several models which are presented in the following. This paper starts from the need to solve problems of information flow and access control to data in an organization, while the structure the organization is not defined and the actual capabilities of its members are not known. Solution to create members' access to organization's documents, data and information is based on trust. This article complements previous studies concerning the possibility of document security implementation, controlling the information access rights in virtual environments based on Web technologies.

1. Problem Statement

Virtual environment based on web technologies, allows the impersonal interaction between various users, knowing each other or not, being part of a real or virtual organization.

Over time, there have conducted various researches regarding data security and privacy assurance systems, such as

- Bell – LaPadulla system (D. Elliot Bell, 1973);
- "Lattice" based system, designed by Dorothy E. Dennis (Denning, 1976)
- Doctoral thesis "Formalising trust as a computational concept" , (Marsh, 1995)
- Role based access model (Ravi S. Sandhu, 1995).
- EPAL (Enterprise Privacy Authorization Language (IBM, 2003; the version submitted to the W3C)
- XACML developed by OASIS (OASIS, 2005)
- "Control Access To Information By Applying Policies Based On Trust Hierarchies" (Marcel DANILESCU, 2010)
- „Assurance model behaviour in social networks based on trust" (Adomnicai C., 2011)

[1]Technical University of Moldova, Faculty "Computers, Informatics and Microelectronics",Chisinau, MD-2004, Republic of Moldova , Ștefancel Mare Av., 168, (+37322) 509-905+40721042950, e-mail marceldanilescu@hotmail.com

2. Introduction

In any type of organization (real or virtual), tasks that have to be solved are generally attributed to people who are grouped according to various criteria, but more often on competence, ability, benevolence, etc., and on each group, the multitude of tasks is also allocated on criteria similar to those that led to the creation of groups. For example, in the virtual environment *OpenOffice.org*, *LibreOffice*, or any community of *sourceforge.net*, we find working groups for: help-desk, design, coding, testing, help systems, user support, documentation, localization and translation, creating sample content, developing tutorials, developing template documents for applications, and many other types of work.

This structure based on working groups, which have a management group, assumes a hierarchical organization, both at the organizational level and at group level,top being provided by the initiative group or entrepreneurs. To access to an organization, any member should receive the member's trust - mainly members of the top group - so it can carry out the tasks assigned and has the power, goodwill and other features necessary for the completing the task.

In the last 20 years, there has been research on trust which can be given to the various groups and their members in the group. (Marsh, 1995), (Roy J. Lewicki, 1998)

In the literature, the maximum given trust is "Blind Trust" with value 1, and the minimum given trust is "No Trust" with value 0. (Marsh, 1994). Based on those mentioned above, we consider that assigning full trust to a person or group, they enjoy the same trust as the person or group who gave it, and the lowest confidence value means that there is no trust.

Between those two values, it can be created a trust hierarchy, based on trust levels.

This way of quantifying the trust granted to a user or user group, help us to determine access and action rights on the files (henceforth called *objects*) in a virtual environment.

In practice, not all objects have the same importance for a user or group of users, because each one covers different topics, more or less important to them. Therefore, we can say that, for a category of users the object is more important while for others it is less important, which makes an object to be necessary for a certain user and unnecessary for other. Also there may be objects that need to be provided with higher or lower trust degree towards a user or group of users

3. Concepts and terms

Generally, trust granted to a person (Marsh, 1995) to perform an action within a group is based on various criteria such as:

- reputation

- competence
- loyalty
- experience
- goodwill
- courage
- Etc.

These characteristics are part of the baggage that comes and departs an organization member. Of course they are not fixed, but evolves with how they participate in the life of the organization. Also these criteria are not fixed for all organizations. For example, while some of them require accuracy, speed work at the expense of experience, and goodwill, others might require from their members loyalty and discretion. Depending on the requirements, criteria necessary for the application of a trust policy are adaptable, each organization creating their own principles and methods of evaluation and promotion of its members.

Further, we will analyse a theoretical model of applicability and enforcement of the access policies based on trust. To create access control policies for users of virtual storage, we must define the following:

- Assessment requirements
- Objects;
- Object Group;
- Life cycle or lifetime of an object;
- Users;
- Users Groups;
- Domains;
- Trust level corresponding to an action;
- Requirements for establishing the trust level;
- Trust level granted to a user for a specific domain, or to one or more objects of the domain;
- Trust level granted to a user group within a group of a domain.

The **object** is a homogeneous and unitary entity of information on electronic support, on which the action is carried out to achieve the purpose for which it was created.

Object group represents a collection of objects that belong to a domain.

Generally, it is difficult to identify and determine that an object belongs strictly to a group or another.

May encounter situations where an object may belong to several fields. For easy distribute objects in groups, we consider that the object belongs to the domain that has the most interaction with it and eventually end object lifecycle.

Groups of objects may have inside a hierarchical organization; some objects arising from end of life on another object.

Object life cycle (duration of existence of an object) represents all the stages of an object, from creation to archiving or deletion.

The user is the person who interacts with objects during their period of existence and performs different actions.

User group consists of people who interact with a set of objects in a domain.

Domain of activity is part of the activities performed, grouped by common charcteristics, such as technical knowledge, economic or scientific common interest, scope, etc...

Definition: We call a **trust value** granted to an action, a value between 0.00 and 1.00 corresponding to actions taken on an object, according to the competences necessary for enforcement action.

Requirements needed for trust value determination are an arbitrary set of conditions which a user must meet to be granted with a certain trust value in order to execute actions.

Trust level is permission granted to a user or group of users to interact with an object or several objects from certain area of activity and to perform specific actions corresponding to the **trust value**.

To create a logical mechanism to control access to objects, we formalize the principles outlined above. For this, we make the following considerations about the elements with which we work.

We define a hierarchy as a finite set of values ($H_1 \leq H_2$) ascending ordered.

We define a sub-hierarchy ($I_1 \leq I_2$) as a sub-set of a hierarchy ($H_1 \leq H_2$) if ($I_1 \leq I_2$) $\subseteq$ ($H_1 \leq H_2$).

Between objects and user interaction is possible, that a user can perform certain operations on an object:

- Reading
- Creation
- Writing (update)
- Addition (append)
- Copy
- Rename
- Deletion
- Archiving
- Approval
- etc.

Interaction between object and user we call **action** and note it with a_i. All actions create the set of actions A.

We define a relation (Marcel DANILESCU, 2010) **as a connection that exists between two elements x and y belonging to disjoint sets and that can be expressed as (r, x, y).**

A trust relationship is a relationship that can be quantified by values between 0.00 and 1.00 corresponding to "no trust" to "blind trust".

When **r** = 0, there is no trust relationship between **x** and **y**, and when **r** = 1, trust is complete. Between these two values representing the relationship extreme, can be defined various actions that can be applied on elements, depending on the relationship trust value, applied to a user or group of users, for an item or category of items

Lemma: An action "a" of "x" over "y" can only occur if the value of the relationship between "x" and "y" is equal to or greater than the minimum necessary to enforce the action.

Thus: if $r=0 \vee r<v$ (v = minimum value for which $\exists a$) $\Rightarrow \neg a$, otherwise $r>v \Rightarrow a$.

Therefore, the control of "***a***" actions can be realized according to the value attributed to "r".

If "***r***" has "***v***" value, greater than the minimum required to execute an action, then "***r***" corresponds to all actions whose value is less than or equal to "***v***". If no value is set for "***r***", then „***r=0***".

We propose the following correspondence between actions and trust levels values:

Trust level	Actions
0. 01	a0
0.02	a0
…….	…
0.1	a1
0.2	a2
0.3	a3
0.7	a4
0.9	a5
…….	…
1	a1

Table1.Example of granting trust values to associated actions

These actions applied to objects can be represented as a tree following form. (Adomnicai C., 2011)

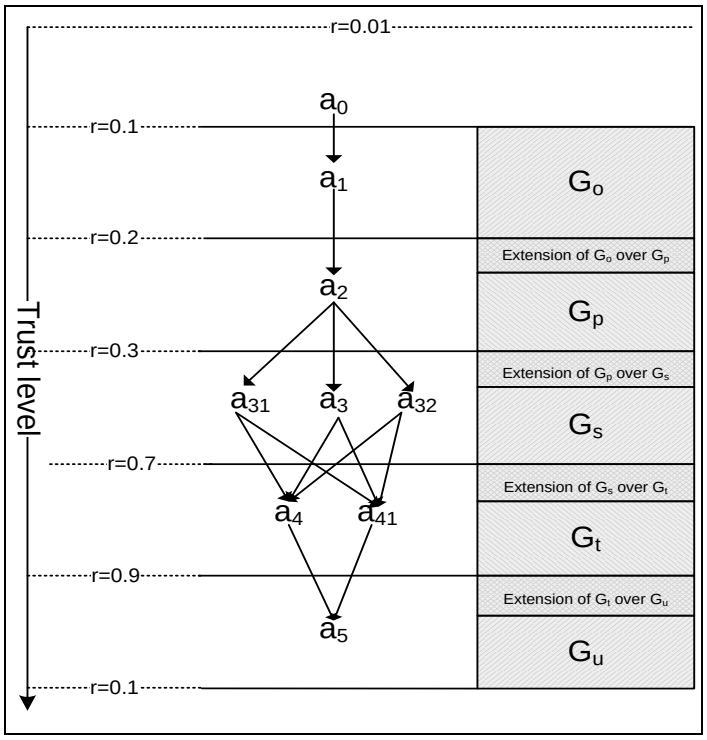


Figure1 The tree of actionsappliedtoobjects

An object or group of objects belong generally to a domain. Depending on the relationship of trust between a group of users (or one user) that belong (belong) to a domain and the group of objects (object) are set the actions they (this) may apply to object. From the above results in the following:

1. Each object is attached to a group of reliable values corresponding to a hierarchy of actions, which is the order of actions which will cover the subject.
2. Each user has a level of confidence in relation to object, depending on which enjoys the confidence to perform actions on the object or group of objects.
3. Right of execution of an action on an object is determined by the value of trust.

This means that it can create a first set of tuples representing the relationship between object groups, user groups and actions based on the level of confidence (GB, D, G, R) on that we call general policy of trust.

Where:

- GO = group objects
- D = domain
- G = Group of users
- R = the confidence level of the group.

Given that an object Oi, which belongs to a group of objects GO_J, in a domain activity D_l ,for a user group G_m has a trust level value R_u , that can only less than or equal to the confidence of the group R_g.

Those are transcribed as:

$$R_u (O_i,D_l,U_n) \leq R_g(GO_j,D_l,G_m)$$

If the in above relationship for users and objects is replaced R_u the confidence level with the corresponding action, we obtain the following tuple: (O_i, D_l., U_n, A_x). In other words, the action A_x on the object O_i is allowed for the user U_n of the domain with the confidence level R_u equal to one level of trust that allows the execution of the action. (Laura Danilescu, 2010)

To simplify allowed actions for an user to an object, we can use only tuple U_n,Au, allowed actions are those that correspond to the appropriate confidence levels. This leads to the attachment of a group of tuples (U, A) to an object. (Laura Danilescu, 2010)

Steps of an object should be recorded as hierarchical sets of tuples consisting of shares and an integer value that can express Vs state of the object (value status). $Vs \in (0,1,2)$ where :

- 0 = unexecuted
- 1 = in work
- 2 = performed

Expression of trust policies applied to a user to a particular object belonging to a particular area, in simplified form, is of the form (O_i,U_n,A_x), and as complete is (O_i,D_l,U_n,A_x).

May be situations where the rights of user groups may not involve the existence of appropriate actions assigned to users in the group. Then you have to establish some restrictions (Marcel DANILESCU, 2010).

Restrictions: We call restriction, limiting the action of an user for an object or category of objects, though he had the necessary confidence level for enforcement action.

To designate a restriction on an action, we note with" -A" a detailed restriction and"-Ru"a set of restrictive policies. Thus we have a set of elements (Oi, A,-Ax) or (Oi, A,-Ru) for the domain D_l.

In general, a restriction must be accompanied by a delegation to another user.

The delegation is reliable transfer made from one user to another in order to carry out actions on objects.

Basic principles applied in trust policy are:

- **generalization** - allows reliable policy of an object or class of documents applied to a user to apply to all members of the group who have the same level of confidence. We say that relation (O_i, U_n, R_u) in a domain D_l, can be transformed in (GO_J, G_m, R_g) or (O_i, G_m, R_g).
- **inheritance** allows that trust policy of a group to be applied by default to one member of the group, unless otherwise is specified. In this case, the policy defined as (O_i, GO_J, R_g) for the D_l can be applied to a user like (O_j, U_n, A_x).

4. Workflow modeling - support for policy implementation based on trust

4.1. Importance of the workflow. Conditions for implementing the access control policy

Creating workflow is very important in order to facilitate the implementation of policies based on trust by revealing of all processes P, flows and levels of confidence in the actions of the various users.

Such an object suffers during life a series of processes ordered according to a plan previously created.For each process corresponds the actions (A), events (E), sequences flow (F) that determines it's semantic. They are executed or are designated to the users.

Each process has a well established position in the workflow of the object, what allow the opportunity to make a hierarchy of processes, which in turn it contain hierarchies of actions (Ak), one of the events (Ek) and flow sequences (Fk).

In determining the processes' flows, are defined the restrictions, delegations, trust levels required by the groups of users of different areas to access and interact with the objects.

The design and the implementation of policies based on trust involves determination of the actions, the events, of the flow sequences, which constitutes each process (P) and their assignment to different groups of users based on their level of trust and the restrictions needed to be applied.

Therefore we can define the conditions needed to apply a policy of trust.

Let be $O_i \in GO \wedge P_i \in \mathcal{P}$ where $P_i=(p_1,p_2,\ldots p_k \ldots p_n)$, and $p_k=H_k(A_k)$ $H_k(E_k)$ F_k

for $\forall A_k$, $\exists(U_k \in G_m \Rightarrow \exists R_u$, $R_u(U_k)=R_a(A_k) \wedge R_u(U_k)=\leq R_g) \oplus$

$\exists(U_x \in G_m \Rightarrow \exists R_u$, $R_u(U_x)=R_u(U_k) \wedge \exists de_v(U_k)$ for $U_x) \oplus$

$\exists(U_x \in G_m \Rightarrow \exists R_u$, $R_u(U_x)=R_u(U_k) \wedge \exists de_v(U_k)$ for $U_x \Rightarrow re_v(U_k) \in RE \wedge \neg \exists re_v(Ux) \in RE$)

Where:

A_k= an action applied to one object;

de_v= delegationreceived froma user $U_{k;}$

DE= the crowd of delegations;

F_k= flow sequences;

G_m= User group of which one user U_k is part;

GO=Group of objects;

$H_k(A_k)$= the corresponding action hierarchyto the p_k subprocess;

$H_k(Ek)$= the corresponding hierarchy of events to the pk subprocess;

O_i=Object i;

P_i=The process applied to O_i;

$p_1..p_n$=numbers of subprocess ale $P_{i;}$

R_u= confidence level of the U user , that is needed for the Oi object;

R_g= confidence level for the GM group;

$R_a(A_k)$ = level of confidence necessary to the enforcement of the Ak action;

re_v=restriction applied to the user U_k;

RE= the crowd of restrictions;

U_k= the user designed to execute the A_k action;

U_x = an userwhich belong to the group $G_{m.}$

From the above we can determine the conditions for the implementation of the different types of access control policies, from the general type, to MAC (Mandatory Access Control) or DAC (discretionary access control).

Definition:We call a policy of type access control generally, a policy that does not include any restrictions and delegation of a user in the time of processing of the objects.

Basically, such a policy is applied in the first phase of creating an organization when there is no history of actions of its members, there were no events which had disturbed the organization, and its members were integrated into the organization on the required criteria applied subjectively, according to opinion made the recommendation received, the result of the interview, proposals, etc.

Its further activities, may then determine how to implement change to the access policies applied, by analyzing events within the organization and with the adjustment of evaluation criteria based on the results obtained.

4.2. Organizational structure and its role in determination of the information flow

Every organization has since its creation, one initiative group, which in time will became the organization's management group. It can be from one to n members, depending on the organization extent, and of those who want and are accepted to join to it.

Depending on their needs, over time, can form working groups as needed, based on expertise, benevolence, etc... Groups can be formed in turn from 1 to n number of members, and which will have an internal hierarchical structure, to solve tasks received or assumed, a structure that can become very complex, at a time.

The appearance of these structures that complement, whereas the organizational structure determines the increase information flow, branching and refining of the operations of the organization, increasing its complexity.

Thus based on its structure, from the first moment, we shall create a graphical structure that represents the actual structure of the organization.

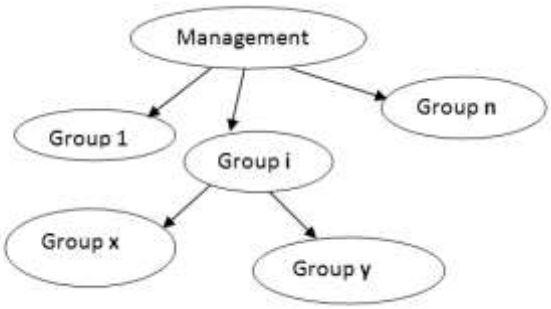
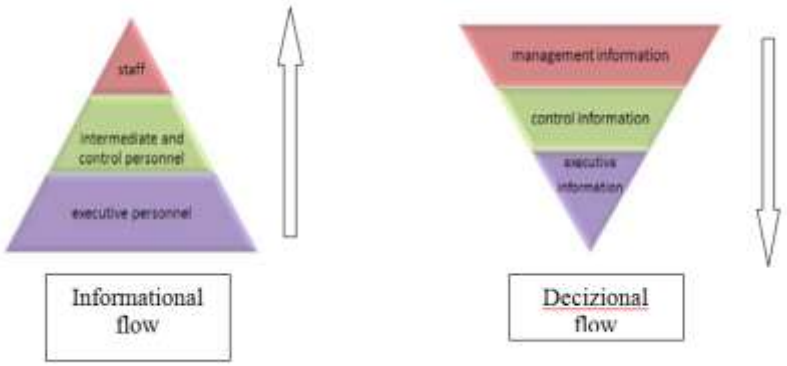


Figure2 The structure model of organization

This structuredeterminesthe mode of action of information flow and activity within the organization, and which will have a great influence on the implementation of access control policies within the organization.

Changing dynamic organizational structure requires the existence of a periodic review of information flow, the importance of the work of members of the organization, how they are involved in theirs activity and the confidence in they, which often involves changing of the position ,of the function, of the confidence, and whether the application of restrictions or delegation of powers. Overall the information flow of the organization has an upward direction, and the decision is generally in downward direction, and is determined by the internal information flow and external information

flow of organization generally behaving like an SRA (automatic system), where control element consists of leadership and the implementation by the ordinary members of the organization.



5. Modelinginformation flow,ways and means

For the analysis and the modeling of the workflow were created over the years, a number of attempts standardization. In the following lines we will make a short presentation of the most representative methods to modeling the workflows and processes.

Workflow Reference Model was first published in 1995 (Workflow Management Coalition, 1995) and is the basis for BPM (business process management) and the software for the analysis of workflow of the systems currently used.

XPDL (XML Process Definition Language) is an XML-based language used to describe a process developed by WfMC (Workflow Management Coalition, 1995). Version 1.0 was released in 2002 and version 2.0 was released in October 2005. The purpose is to store and retrieve a chart XPDL process, to enable to a tool to model a process diagram and to other tool to read and edit the diagram, while other is "running" the process model on the XPDL compliant BPM engine , etc. XPDL is not an executable programming language, but specifically is used to the design of a defined process.

BPMN (Business Process Management Notation) (Object Management Group, 2004) is a standard for modeling the business processes, providing a graphical notation for specifying the processes in a process diagram (BPD), based on a flowcharting technique very similar with activity diagrams from the Unified Modeling Language. Version 1.0 was standardized in 2004. In 2011 was stabilized the current standard, version 2.0. The objective of BPMN is to support business process management for both the technical users and the business users, in the area, by providing of a notation

that is intuitive to business users and is able to represent complex the processes semantics.

With the tools above, you can describe the information flow within an organization, but in terms of describing user of actions in a process of data processing standards, do not provide a specific methodology, but they can be adapted to highlight the actions, events and the stack flows to processing of objects.

5.1. An example of the workflow modeling and processes within an organization

To illustrate the application of a standard for modeling of the business processes, in the following we present the elaboration of the analysis of the models development of the processes to that subject, are the objects, to determine the actions, events and the stack flows , necessary for modeling for modeling of the control access .

First, knowing the internal organization, it is necessary to make an inventory of all objects which are subject to the various processes within an organization.

As a first step for the systematic analysis effort, is necessary to group the objects, based on the field of the activity properly.

After clustering, each object is analyzed. Modeling was done by the BPMN standard.

In the pictures below are summarized these operations. (Figure 3)

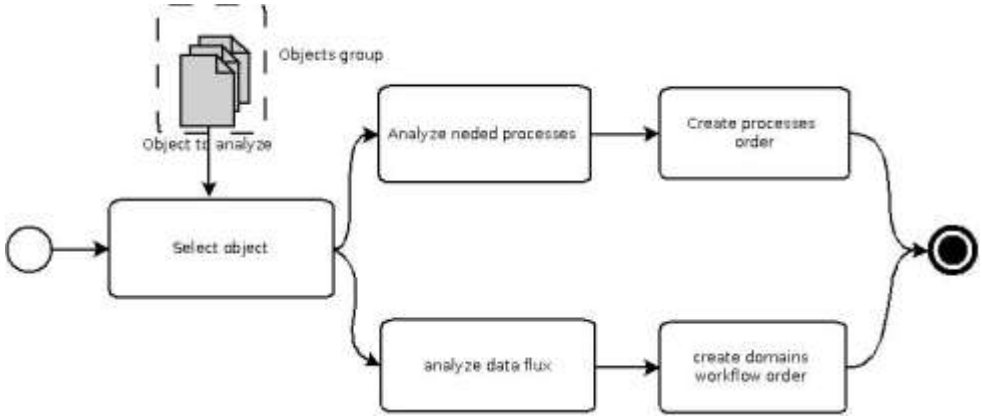


Figure3Objects analyses

Once have been established the required processes of the workflow, that are applied to an object, proceed to analyze of each process in part to highlight the workflow actions of and events related to the subject. (Figure 4)

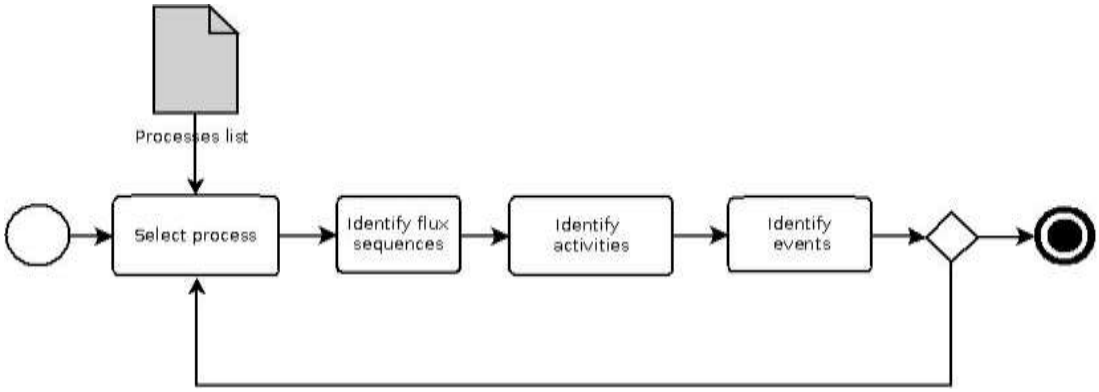


Figure 4. Process analyses

Following the establishment of the actions and events, we will move to the modeling of control of actions, establishing what users will be allowed to perform as actions on the objects. This process is described in Figure 5

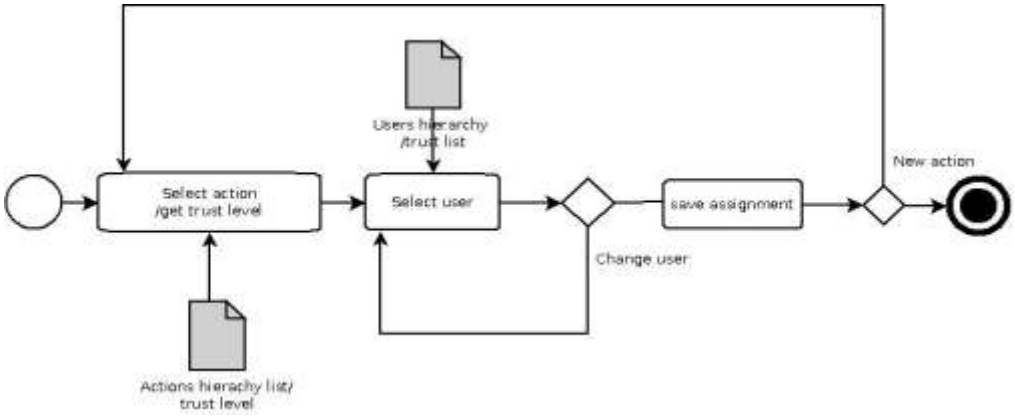


Figure 5. Policy creation

5.2. The restrictions of the policies of trustworthiness , the delegation of powers

Many times it may happen that during the design process, it will be posible to assigned to an user a number of actions that can be executed at a time. (Ex. object filling, printing, transmitting information, and so on).

If at one time, the user is unavailable, then is appointed as delegated an another user, who can perform this actions, and we must to limit the rights of the action of these activities that can were delegated to another user. These restrictions may also apply

when a user loses confidence which enjoyed in the past. This also means assigning the right of the action to another user.

The scope of restrictions and delegation is presented below.

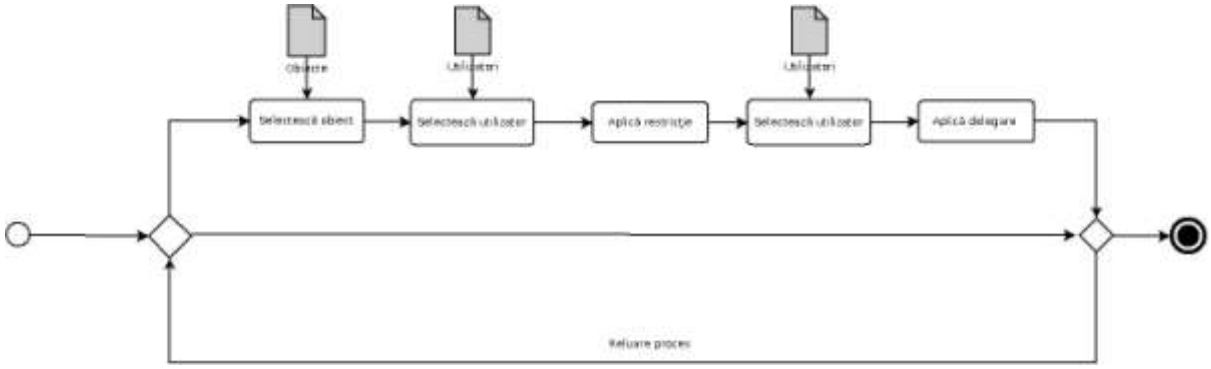


Figure6. Actions to limit and delegate other users

5.3. Trusted policy enforcement in the authorization of actions of the users

The access control systems, authorization of user actions, requires a mechanism permitting and enforcement of access policies created.

Thus, in addition to access centralized applications, this, also creates a mechanism for verification of users which keeps track of of actions permitted, of restrictions and their delegations.

In the following, we describe in brief, the operation of such a mechanism.

A user issues a request to access an action to be performed on an object. To check a user's access to an object, the process will issue a request to the **access controller**. It will consult the **evaluator acces**which will issue a request for the **policy evaluator**.

Policy evaluator consults the **access list of users**, **list of users delegation** and **list of restriction of the users** and seeks information about the user.

Evaluator decisions consults the **policy evaluator** results and returns a response to the **evaluator access**, which forwards it to the **access controller**.

Depending on the response, the user has access or not to a particular action on an object.

User access lists, those of the delegations and of restrictions are created and maintained by security policy administrator.

All this isshown in the figurebelow.

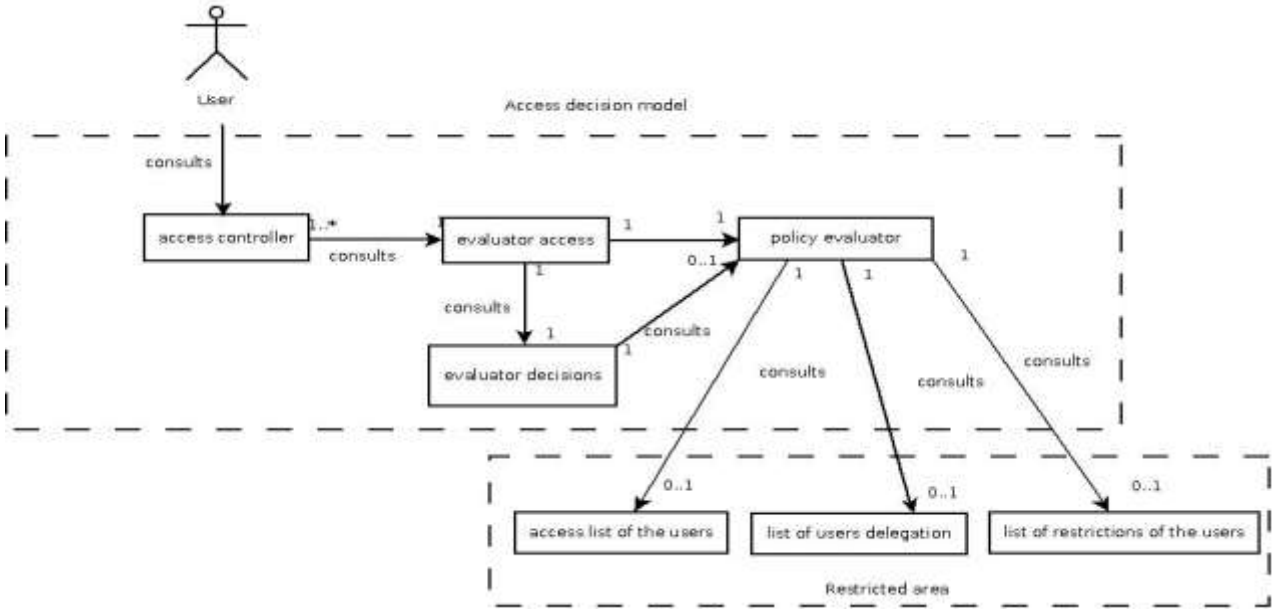


Figure7. Access Decision Model

6. The administrative model

To create a trusted administrative model, several principles should be considered:

• Users involved in the management of access control can not perform activities of coordination, approval, verification which are unrelated to their work;

• A user has created a document can not participate in the activities of validation, approval, deletion, archiving. He can do that, only if has a special delegation;

• Objects that are created by a member of a group that has a high level of trust can not be validated or approved by a member of a group that has a lower confidence level;

This model bellow, essentially describes how to use administrative model for implementing access control.

First list of objectsto be createdand the list ofusers andtheirconfidencelevels.

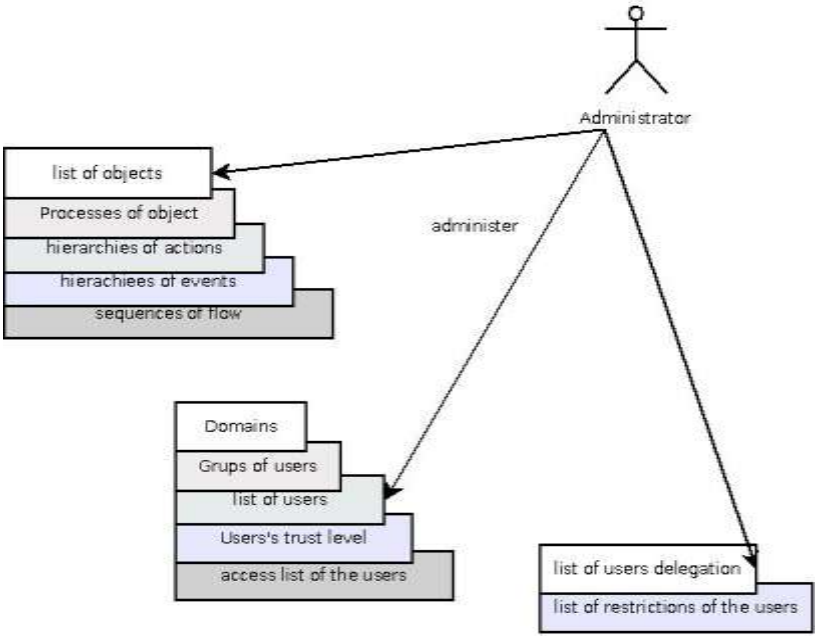


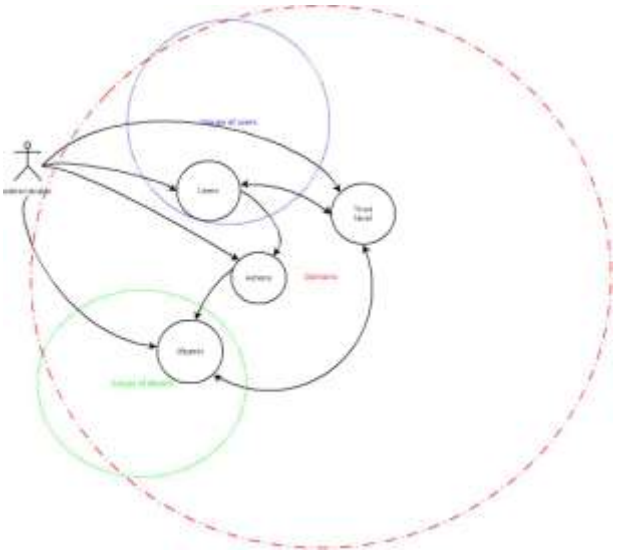
Figure8. Administrative model

Then for each object of the hierarchy there will be recorded the actions and the access assigned to the user .

If an action is required for delegation of power shall be filled in the list of delegations and any restrictions will be recorded in user list restrictions.

In Figure 9 is presented a scheme for managing the access control

Figure9. Scheme for managing the access control



7. Conclusion

For to control the access and the actions of the users within virtual organizations or SME's, it is difficult to create a model with RBAC or other methods, since these organizations are dynamic in structure, with little staff and with no stable functions. In order to model the access control and of actions, we have create this study, study that completes a void in this regard. This paper presents an innovative, easy to implement security method that allows determining the actions applied to the objects by the users.

For the future, we plan to develop a language for expressing access policies and a system modeling based on graphics, which are then translated into XML, for easier interpretation of required policy elements.

8. Bibliography

Adomnicai C. Danilescu M. Assurance model behavior in social networks based on trust [Conference] // 2011 3rd International Conference on Computer technology and Development / ed. IACSIT. - Chengdu, China : IACSIT, 2011. - ISBN: 978-0-7918-5991-9.

D. Elliot Bell Leonard J. LaPadula Secure Computer Systems: Mathematical Foundations [Report]. - [s.l.] : MITRE, 1973. - 2547.

Denning Dorothy E. A Lattice Model of Secure Information Flow [Article] // Communications of the ACM / ed. Robert L. Ashenhurst Univ. of Chicago Chicago, IL. - NY : ACM, May 1976. - Vol. 19. - pp. 236 - 243 .

IBM Enterprise Privacy Authorization Language (EPAL) [Online] // w3.org. - IBM, 2003; the version submitted to the W3C. Available at. - martie 20, 2009. - http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/. - Version 1.2, .

Laura Danilescu Marcel Danilescu Control Access To Information By Applying Policies Based On Trust Hierarchies [Conference] // International Conference on Computer and Software Modeling, ICCSM 2010. - Manila , Philippine : Institute of Electrical and Electronics Engineers, Inc, 2010. - pp. 285-290. - IEEE Catalog Number: CFP1093L-PRT ISBN: 978-1-4244-9095-0, IEEE Catalog Number: CFP1093L-ART ISBN: 978-1-4244-9097-4.

Marcel DANILESCU Laura Danilescu CONTROL ACCESS TO INFORMATION BY APPLYING POLICIES BASED ON TRUST HIERARCHIES [Conference] // Conferinţa internaţională”Educaţie şi Creativitate pentru o societate bazată pe cunoaştere” 2010. - Bucureşti : Universitatea Titu Maiorescu, 2010. - pp. 49-54. - ISBN 978-606-8002-47-7.

Marsh Stephen Paul Formalising trust as a computational concept [Book]. - Stirling : Dept. of Computing Science and Mathematics, University of Stirling, 1995.

OASIS eXtensible Access Control Markup Language (XACML), Version 2.0 [Online] // www.oasis-open.org/committees. - Version 2.0; OASIS Standard, February 1, 2005. - 2009. - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml..

Object Management Group About the Object Management Group [Online] // Object Management Group Web site. - 11 1997. - 2009. - http://www.omg.org/gettingstarted/gettingstartedindex.htm.

Object Management Group BPMN Information Home [Online] // Object Management Group - Business Process Model and Notation. - May 3, 2004. - 2009. - http://www.bpmn.org/.

Ravi S. Sandhu Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank Role-Based Access Control Models [Article] // IEEE Computer / ed. press IEEE. - NY : IEEE Press, February 1995. - October. - Vol. 29. - pp. 38-47.

Roy J. Lewicki Daniel J. McAllister and Robert J. Bies Trust and Distrust: New Relationships and Realities [Article] // The Academy of Management Review - Stable URL: http://www.jstor.org/stable/259288. - [s.l.] : The Academy of Management Review - Stable URL: http://www.jstor.org/stable/259288, July 23, 1998. - pp. 438-458.

Workflow Management Coalition XPDL Support and Resources [Online] // Workflow Management Coalition Web site. - 1995. - 2011. - http://www.wfmc.org/xpdl.html.

Workflow Management Coalition Workflow Management Coalition Home [Online] // Workflow Management Coalition Web site. - Workflow Management Coalition, Jaqnuary 19, 1995. - 2010. - http://www.wfmc.org/reference-model.html#workflow_reference_model.