Organization's data access control policies based on trust

Laura DANILESCU[1], Marcel DANILESCU[2]

[1]Lecturer drd., Danubius" Univeristy Galaţi, Faculty of Economic Sciences, ldanilescu@univ-danubius.ro;
[2] IT Manager,drd., ASWIC Ltd., marcel.danilescu@aswic.ro

Abstract

Circuit information in an organization involves the creation of documents whose content contributes one or more employees. Documents beneficiaries may be managing board, individuals, working groups or departments. Because these documents have to be safe in terms of confidentiality should attach them an access policy. This policy is based on providing trust levels of both staff and documents. Access right results from the algorithm which compares the two trust values.

Keywords: privacy, trust hierarchy, trusting authorization policy

1. Introduction

In the context of increasingly use electronic data on trade, business or research, in education administration, etc. and in the context of new paradigms such as: e-commerce, e-government, e-administration, e-payments, e-learning, etc., appears essential to establish a reliable framework for Data Exchange between organizations, departments and users.

For the overwhelming majority of successful organizations, information and information technology are the most important values. Databases, financial information, accounting data, employee profiles and many other documents form the core processing of estimates and business plans, resulting in the final steps of a business future in a very dynamic market.

Companies now understand that to be competitive, you must receive process and send information rapidly and securely to all partners. Meanwhile, the opening to the outside brings with it many risks that modern management should assume together with efforts to minimize them. But as the communication process is always undertaken in both directions, the dangers come not only from the outside.

A ***threat*** to the computer system may be: one person, one program or one event that could cause damage or destruction to the system. Those threats can be malicious (such as the intentional modification of sensitive information) or unintentional (such as accidentally deleting data).

Vulnerabilities are system weaknesses that can be exploited by threats. For example, unauthorized access to system resources can be obtained by a foreign person by guessing the password. The vulnerability exploited in this case is the choice of weak passwords by legitimate users of the system. Reducing or eliminating existing vulnerabilities can reduce or eliminate the risk of threats.

A threat example is ***compromising data privacy*** – it occurs when an unauthorized person get in possession of confidential data to the organization. Compromising privacy occurs when data is accessed, read or given to a person who has not this right. This occurs when someone gains access to confidential information not protected by appropriate cryptographic mechanisms or printed on paper.

The main ***vulnerabilities*** that can be exploited for this purpose are:

- Improper setting access rights to files containing confidential information
- storage / transmission of confidential information without being encrypted,
- storing backups in places poorly protected
- printing of confidential information on network printer and improper handling of these copies.

According to researches, 56% of employees come into contact with confidential information abandoned on printer and 51% of respondents are unaware of the existence of processes and technologies in their company to provide protection for printed documents.

Those working in the financial / banking has the best chance to come into contact with confidential documents; more than two thirds (68%) of respondents stating that observe such documents when are listed.

2. Problem statement

The research question is to access a document based on political restrictions imposed by authorizing of a trust level determined based on hierarchy. Hence the problem of defining a policy for authorizing access based on trust levels associated with both documents and users;

Documents are available:

- at some point
- to a particular user
- on a given machine

3. Concept and terms

3.1. Trust within the organization

***Trust** is a universal concept and makes in any context, positive effects. Most commonly used definition of trust in scientific contributions is given by Mayer, Davis and Schoorman (1995): "The consent of a party to be vulnerable to the actions of another party, based on the premise that this party will take some significant action for the one who gives trust, regardless of ability to monitor or control the other party.*

In the structure of relations within the organization and relationships between organizations, where the performance takes place using information and communication systems and where player's behavior is influenced by social restriction and formalities should be given attention to different types of trust:

- personal trust: actor has the experience and appreciation of its intention to build, with a strong sense of safety, the dependence of another person or group of persons, being aware of possible negative consequences. For this intention is evaluated in advance a person's confidence level.
- impersonal trust: it is the expectation that a system or institution to permit a positive future development. The system is evaluated before being trusted.

"Trust is the intention to act as individuals or impersonal systems behave in the manner expected and provided. These expectations are based on experiences and the actor is aware of the risk involved. "

The importance of trust in corporations and networks based on a hierarchical structure or a structure based on different groups, has sparked interest both in economic practice and economic literature.

In traditional business, trust is influenced by formal or organizational hierarchy. Measures to form a potential network represent a reliable research.

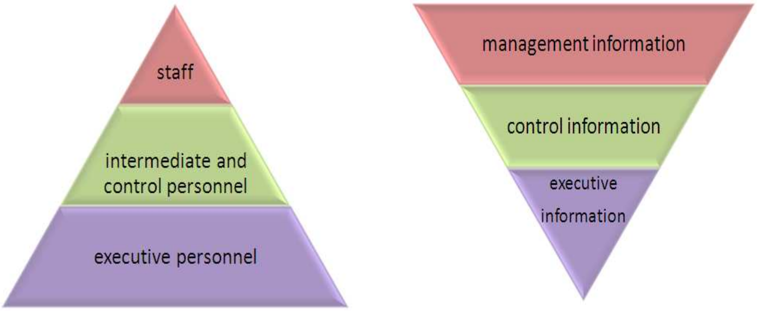
3.2. Data and information within the organization

Every organization has a pyramid organizational structure, personnel decisions are at the top of the pyramid, and the execution is at the bottom of the pyramid.

To take the best decisions, decision staff must have access to as much information and data that will underpin the management policies, while executive staff does only need data and information that they can use in processes currently taking place in the organization.

Also, data and information quality is different; top staff with access to data and information sensible that can determine the fate of the organization, unlike the execution staff that has access only to data and information needed for their activities current base of the organization.

Based on this model, it can be concluded that people who have access to data and important information contributing to the management policies are top people in the organization pyramid, which leads to the following chart:



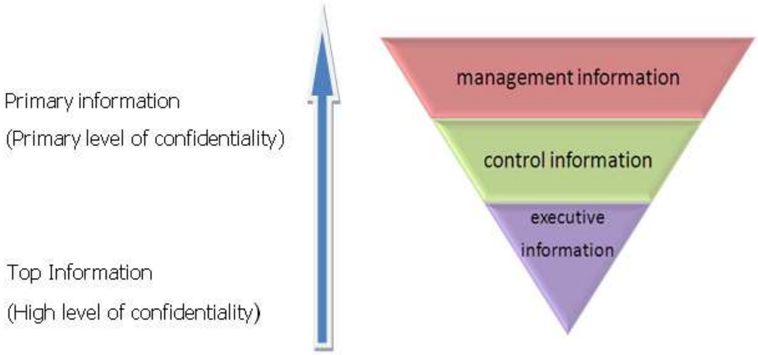
From these diagrams one can see the following:

Executive staff is the largest unlike management and is inversely proportional to the quantity and quality of information circulating within the organization. Risks of reversal of roles in terms of information management is very high and can only lead to substantial losses of the organization in its operations because the winners in the modern economy are those organizations that respond quickly to the market changes and they do a good information management .

Information management is not creating a central database with data or knowledge of a company. Information Management is the technological foundation that unites these people and enables them to work as a team for the smooth running of activities of the organizations. Therefore, the organization's information needs are different, which leads to the need for the creation of information policy.

Information requires protection, to prevent sensitive data disclosure at levels that are unable to process and keep data privacy. Therefore, data privacy policy is very important within the organization.

In general, at all skill levels within the organization are produced, consumed and stored information as part of its information flow. Level of refinement and privacy requirements of information increases as they are for higher levels of competency. Therefore, we can make the following diagram showing the interdependence between the level of competence and the necessary of confidentiality of information, taking into account the degree of refinement of information, which is closely related to management act.



A lot of organizations have implemented security or privacy policies through classified documents. However, this does not solve the problem of a unitary report within the organization and expanding the disclosure of confidential data, according to the hierarchical level that a person occupies within the organization. There are also situations where a person, even if occupying a top position in organization, may not be considered reliable, and certain information should have a greater level of privacy to be protected. This means that a person can not access certain information because it does not have a sufficiently high level of trust within the organization.

4. Solution Approach

4.1. Trust hierarchies

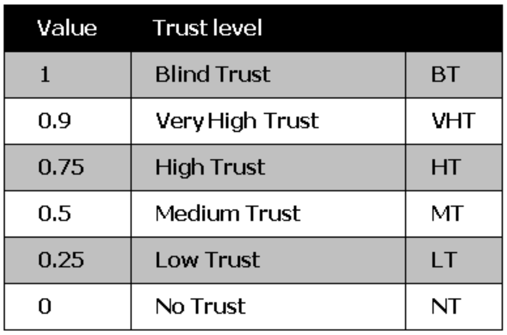
An organization consists of a number of members involved in achieving a particular purpose. In general, any organizational structure is a hierarchical type structure, which is a leader and members to execute various activities under his directions.

Organization does or does not trust the people involved in information-decision process within it. Information-decision process is manifested by the creation of documents containing data and information that are processed by individual (called subjects) belonging to the organization.

Trust is manifested by allowing access to various data and information, according to the position *subject* to that information. *Subjects* may thus acknowledge, change information, to quote, modify, etc. or do not have access to them.

Subjects are part of various working groups, formal and informal. Formal groups are those that form the organization (departments, services, departments, offices, workshops, etc.) and informal groups or instant groups are created for a certain project and outgoing from achieving the goal. During the activity of these groups (formal and informal), access to objects or classes of objects stored, created or used, is based on trust given by the organization to each topic that is part of a group. Granting trust is differentiated, depending on the *subject's* position, activity and importance within the group (formal/informal) and the organization.

There may not be a simplistic approach to these levels of trust, such as *allowed/deny* (*trust /distrust*). Sociology professionals have determined that the trust level takes fuzzy values, i.e. values between 0.00 and 1.00, values which have roughly assigned corresponding levels of trust. Levels correspond to ranges of values presented in the table below:



Value	Trust level	
1	Blind Trust	BT
0.9	Very High Trust	VHT
0.75	High Trust	HT
0.5	Medium Trust	MT
0.25	Low Trust	LT
0	No Trust	NT

In general, the top level of an organization receives the highest level of trust and the execution receives the lower trust level, in direct proportion to the importance of the work within the organization.

4.2. Assigning trust levels

There are two categories of trust levels:

– The local trust level (is the level of the Working Group);

– The global trust level (is the level of the organization).

This can be seen directly in the following example:

X belongs to a working group and it has to create a report on a situation at a time. X is also a member of a formal group which trust level is MT, but has been taken in a working group which should create a document whose trust level is HT.

At the organizational level, X trust level can’t be increased to HT, but X have BT level for his part of document, which is contrary to its general level. Therefore, the document will be divided in parts (objects, classes of objects), some to which X may have the BT level (author, co-author) and some to which X might have the NT level. Generally, apply the NT level if the difference value between the SL (subject trust level) and the OL (Object Level) are equal to or less than zero. In other words, if the subject's trust level is lower than the level of trust required to access the object.

$$NT <= SL\text{-}OL \leq 0$$

In this way groups of objects can be created by groups of subjects that can then be assembled and presented. But each of those who access the final object will have access to only those objects that meet the above inequality.

To implement this policy of securing data and access to them, was created TAP (Trust Authorization Policy).

4.3. Trusting Authorization Policy TAP

TAP (Trusting Authorization Policy) is a mechanism for implementing trusting policies within organizations.

4.3.1. TAP Objectives

- To codify trust levels of organization
- To create security policies of data and information;
- To be flexible and easy to implement, regardless of platform;
- To be easily understood and maintained;
- To enforce the necessary trusting policy;
- To be platform independent.

A TAP is a set of rules applied by a user of to a class of objects with a purpose.

Objects during their lives, go through four stages:

1. **Creation stage**. The stage at which an originator creates the object and the object is classified as "private".
Initiator's private key encrypts the object and sends it through the chain for verification, completion and approval. At this stage, it is proposed to apply generally trusting level to the object and its constituents. Subject receiver opens it with the originator's public key, and will check. If it considers that to be changed, it will send to the originators encrypted with his private key. The receiver will complete the object, if necessary, with other elements that will also have trusting levels and than send the encrypted object through the chain that serves the approval of the object.

2. **Approval and classification stage**. Final receiver of the object, which acts for its approval, receives the object and approves the trusting level applied to the object and its constituents. This moment can be considered the enforcement moment of TAP. Since then, the subject may be:

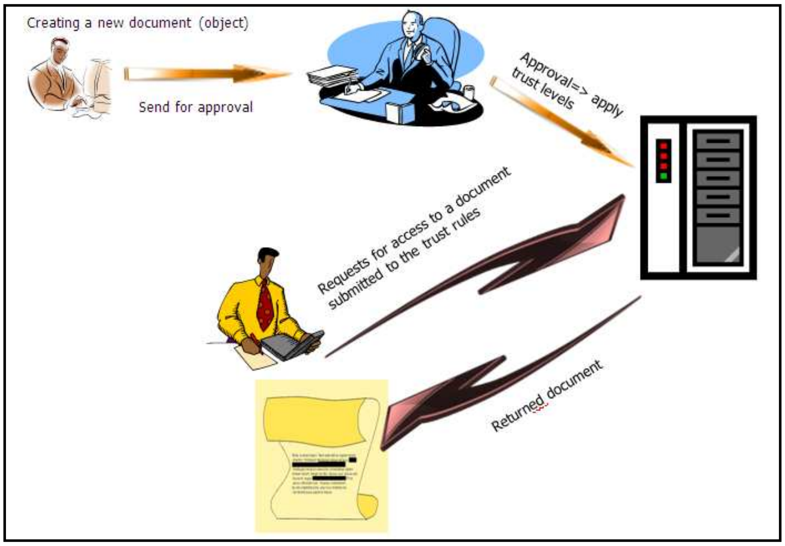
a. *Public* **-** access from inside and outside organization (partners)

b. *Trusted* **-** have access only subjects belonging organization

c. *Archived* **-** no one longer has access without approval

3. **Publication stage**. Depending on the object, it can be *public* or *trusted*. In both cases, the policy applies to the object and constituents, and only if it is *trusted*, it can be accessed by only organization members.
4. **Archiving stage**. The object is archived for future consultations.

The following is a document circuit on which applies trusting policy.


Creating a new document (object)
Send for approval
Approval=> apply trust levels
Requests for access to a document submitted to the trust rules
Returned document

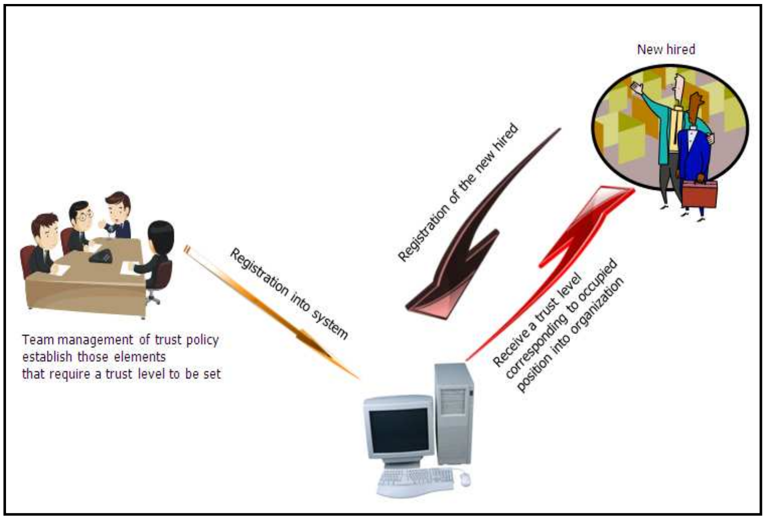
4.3.2. TAP implementation rules

Trusting manager or delegated person applies this policy as board decisions.

Any change in the document will be logged, and may be used only with permission of the head board or delegated person, who will confirm the trusting policy.

Trusting manager or his delegated person has access to the categorization of objects and objects which are subject to the trusting policy, but can not access the content unless specially authorized to have access to them.

The figure below illustrates the role of the management team in allocation of trusting levels for both users and objects.


New hired
Registration of the new hired
Registration into system
Team management of trust policy
establish those elements
that require a trust level to be set
Receive a trust level corresponding to occupied position into organization

Trusting actions must comply with policy decisions and applicable trusting policy:

- Read,
- Quoting,
- Comment,
- Printing,
- Amendment, Supplement,
- Establish
- Approval

For verification of application actions, policy validator will check their compliance with any change in status to a category of objects, object or subject.

Any subject in the TAP can not change policy without the consent of trusting person board. Policy change may be made only on request when the situation demands.

Any formal or informal group which is involved in the process of creating and operating trusted documents will be responsible for approving a temporary member of the group activity and will be marked as head of the group.

Trusting policy change may be permanent or temporary and will be logged.

5. Conclusions

For an organization, information is one of the most important values. Databases, financial information, accounting data, employee profiles and many other documents form the core processing of estimates and business plans, resulting in the final steps of a business future in a very dynamic market.

A company to be competitive should receive process and transmit information quickly and securely to all partners. Meanwhile, the opening to the outside brings with it many risks that modern management should assume together with efforts to minimize them. But as the communication process is always undertaken in both directions, note the only dangers come from the outside.

Reporting needs of the organization are different, which leads to the need for the creation of information policy. Reporting needs requires also information protection to prevent the sensitive data disclosure at levels of competence that are unable to process and store such data. Therefore, is very important the privacy policy which complements the security policy for information circulated inside the organization.

Regarding data access control, it can not be a simplistic approach to the type of access rights such as *allowed/deny*, or in other words, *trust/distrust*. Therefore, research topic, by refining the approach to define hierarchies on access rights based on trust brings a new model for security of information conveyed by the organization, substantially improving reporting needs of all levels.

6. Future Work

The reason of research is to provide a mechanism to add new features to protect XML documents. Thus, will be proposed a XML-based language to specify ***trust policies*** to be enforced to XML documents.

7. References

Prof. univ. dr. Dieter J. G. Schneider, M. F. (n.d.). "***Importanţa Încrederii În Cadrul Companiilor Virtuale***". Universitatea din Klagenfurt, Austria , 40-46.

Roy J. Lewicki - Ohio State University, Daniel J. Mcallister, Robert J. Bies - Georgetown University , "***Trust And Distrust: New Relationships And Realities***", Academy of Management Review 1998. Vol. 23, No. 3,438-458.

Dasgupta, Partha (2000) '***Trust as a Commodity***', in Gambetta, Diego (ed.) ***Trust:Making and Breaking Cooperative Relations***, electronic edition, Department of Sociology, University of Oxford, chapter 4, pp. 49-72

D. Harrison Mcknight, Larry L. Cummings, Norman L. Chervany, University of Minnesota--Curtis L. Carlson School of Management, ***„Trust Formation In New Organizational Relationships"***