Trusting Policies, a New Instrument for Data Protection in Business Reporting

Senior Lecturer Laura Danilescu, PhD in progress
Danubius University of Galati,Galati, Romania
ldanilescu@univ-danubius.ro

Abstract: Controlling access to data and information within organizations is an important concern today and also our aim. This paper is based on the concept of trust, which allows access control and control of actions that can be applied to data and information in documents held in computer systems. Methods we have used are: defining trust and assigning trust levels. Results we have obtained are trust policies based on trust hierarchies.

Keywords: trust; document; privacy; trust hierarchy; trusting authorization policy

JEL Classification: H30; L80; L89

Business Reporting

A growing number of companies use the Internet in the replacement of written reports on paper. These organizations built intranet, extranet networks, and their own sites in an effort to help employees, businesses and other partners to access the reports of the company. (1)

Development of Internet-based reporting is problematic for entities involved in reporting (reporting organizations, internal financial services, financial community) who have their own reasons and intentions for gathering and storing information, but all require rapid and standardized communication. Development of Internet technologies has had a large impact on organizations and in the near future impact may increase with the introduction of a standard reporting language based on the Internet. (1)

Business reporting is defined as "public reporting of financial data and operating a business enterprise." Business reporting is generally divided into two types:

External reporting: for business partners; involves spreading a selection of information from the records (financial and nonfinancial) of an organization.

Internal reporting: for management; contains periodic information required to control and drive the business.

Pragmatic and social world can be linked directly with partners, which, for decision-making intention, should be able to access information anywhere, anytime and under certain conditions.

Thus, it seems essential to establish a trusted framework for reliable data exchange between organizations, departments and users.

For most organizations, the interest in computer security is proportional to how they are perceived threats (2) and vulnerability of the information systems (3).

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 are cores of estimates and business plans, resulting in the final steps of a business future in a highly dynamic market.

Companies now understand that to be competitive, you must receive process and send information faster and more secure to all partners. At the same time, this openness to the outside brings with it many risks that modern management should assume with the effort to minimize them. But as the communication is always two-way, threats come not only from the outside.

The role of a program that implement and ensure a certain degree of information security in a company, is to reduce and keep under control the level of risk to which the company is exposed. Risk level is close to zero only by reducing system functionality and making major investments in security technologies. The organization management shall be the one who decides the level of acceptable risk and the value of the investment to secure the system, so that the ratio of these values to be balanced financially. The objective is to determine the equilibrium in which the costs are minimal compared to the level of security desired.

A ***threat*** to a computer system may be a person, a program or an event that can cause damage or destruction of the system. These threats can be malicious in nature (such as intentional modification of sensitive information from the system) or accidentally (such as accidentally deleting data). They are also considered threats, natural disasters such as floods, earthquakes, fires, etc.

Vulnerabilities are weaknesses of the system that can be exploited by threats. For example, unauthorized access to system resources can be obtained by a foreign

person by guessing a 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.

Security Service is the collection of security mechanisms and procedures that helps to protect the system against specific threats. For example, authentication service helps to protect the system against unauthorized access to resources by identifying users who require access to the system. Integrity and confidentiality services help to protect confidential data within the system.

Trust between business partners

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 behaviour 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.

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*) (4). Sociology professionals have determined that the trust level takes fuzzy values (5), 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:

Table 1 Trust levels

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.

The document built on the concept of "privacy and trust"

This concept arose because of observations on the need for information both intra and inter-organizations, access to various documents for all members.

From the first observations we can see that how to access a document is fairly simplistic ('allowed' or 'deny'), which may lead to a lack of information to the user who wants to access a document, but because the document contain prohibited information for this, it cannot access any information that is entitled to access. Yet, the documents contain both public information, and information that are subject to varying degrees of confidentiality based on the confidence enjoyed by the person who has access to them.

Also, to access data and information through the two previous methods, the user must be connected to the organization network and can only see online, while the new solution proposed here allows the document to be consulted both on-line and off-line.

Suppose that is made a report to be circulated to all staff, shareholders and business partners. Each of these categories and category members are in different "trust" relationships with the organization. Therefore, everyone has access to the public part of the document and also each of them has access to certain confidential information under the policy of "trusting" of the organization.

Therefore, if the organization has 1,000 employees, 10 shareholders and 25 partners, should be made a minimum of 1035 of various documents to enable everyone to have access to both document and data tailored to the policy of "trusting ".

The new system proposed here, allows to create only one document processed by each employee, according to the "trusting" policy, and to reveal only the information that has right of access.

Thus, each department will create part of the document which will be part of the whole. Then it apply the "trusting" policy on the part of the document and submit the document with the policy applied, which will make confidential data to not be

seen by those who are not allowed. Then the document will be assembled and distributed. Each of the receivers will use keys that allow them to open various parts of the document. Thus, each read only what is allowed to read in the document. Therefore, it is created a unique document that will meet the organization's privacy policy.

Assigning trust levels (6)

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).

Trusting Authorization Policy TAP

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

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, 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.

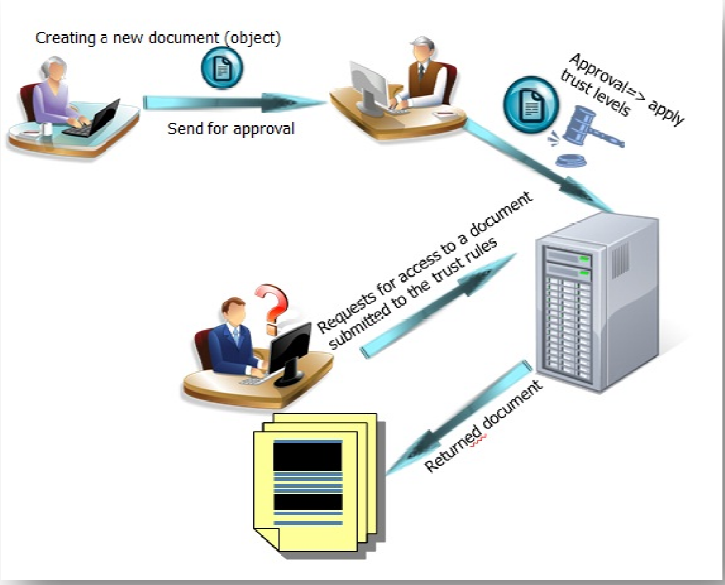

Figure 1 Trust policy applied on a document

Conclusions

Considering that Network and Information Security became a priority for most enterprises, TAP comes like a good instrument for writing enterprise privacy policies to govern data handling practices in IT systems.

Bibliography

Ghilic-Micu, Bogdan & Stoica, Marian (2004). *Organizatia Virtuală/Virtual Organisation.* s.l. Bucharest: Economică, 2004, pp. 207-211.

Bishop, M. (2005). *Introduction to Computer Security*. s.l. Addison-Wesley.

Bocij, P.; Chaffey, D.A.; Greasley, & Hickie S. (2009). *Business Information Systems.* s.l. Financial Times, Prentice Hall: An imprint of Pearson Education.

Lewicki, Roy J.; Mcallister, Daniel J.; Bies, Robert J. Trust and Distrust: New Relationships and Realities. s.l. *Academy of Management Review* 1998. Vol. 23, No. 3, 438-458, 1998.

Harrison Mcknight, D.; Cummings, Larry L. & Norman L. Chervany. *Trust Formation in New Organizational Relationships.* s.l. University of Minnesota--Curtis L. Carlson School of Management.

Danilescu, Laura & Danilescu, Marcel (2010). Control Access to Information by Applying Policies Based on Trust Hierarchies, 2010 International Conference on Computer and Software Modeling, ICCSM 2010 – Manila, Philippines, Publisher: Institute of Electrical and. *Control Access to Information by Applying Policies based on Trust Hierarchies.* Manila, Philippines: International Conference on Computer and Software Modeling, ICCSM 2010.