ACL-BASED MODEL FOR USER ACCESS CONTROL IN MANAGEMENT APPLICATION PORTALS

Florin Răzvan Lupşa-Tătaru, PhD Student, Vladimir Mărăscu-Klein, Prof., PhD, "Transilvania" University of Braşov

Abstract: In management application portals, each application has specific features that reflect in continuous updates of information with which it works. The information may have a higher importance level or less and can be classified, and hence, users may be classified, resulting in the need of a control system for information access. The paper aims to present a model of controlling user access to information based on access control list (ACL).

Keywords: ACL, model, access, management, portal

1. Introduction

The need of user access control became an important aspect in every commercial or non-commercial entity management application portals because of the sensitivity of knowledge stored. In many such entities, internal users have access to all or most of the critical information regarding partner's data, accounting information but also strategic management information.

An **access control list (ACL)** is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.[1]

A **computer security model** is a scheme for specifying and enforcing security policies. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, or no particular theoretical grounding at all.[2]

Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.[3]

A management application portal is a gateway that unifies access to all management information and management related applications, usually on an intranet.

2. ACL-based model

All applications part of a portal can be considered as layers on information stored as shown in figure 1. Therefore the control of users access to information must take into

[1] http://en.wikipedia.org/wiki/Access_control_list
[2] http://en.wikipedia.org/wiki/Computer_security_model
[3] http://en.wikipedia.org/wiki/Security_policy

consideration the information importance level and implemented both through portals control systems and each applications control system.

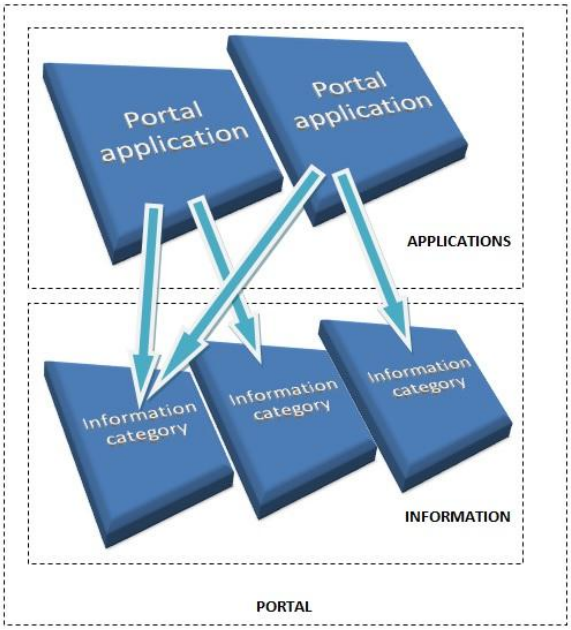

Figure 1. Applications as layers to information.

Creating an ACL-based model for user access must take into consideration some aspects which an portal administrator must control:

- What information is stored, what is the importance level of each information and how can it be classified
- Which users can access what information or information category and what operations can they perform on the information
- How can users be grouped based on information categories and operations beeing performed

The classification manner of the information in terms of access may differ from the perspective of applications compared to ACL models perspective. For example, the information belonging to human resource management can be classified in terms of applications taking into consideration organizational structure of the entity, but in terms of ACL model this may not be respected, a person on higher management level could have fewer access rights to some information compared to a person on a lower hierarchical level.

Creating an ACL model can be done following the next steps.

A. A good starting point in creating an ACL model for user access control is to create an access role for each information category. A role is a conceptual term, a routine that can be seen as a task or set of responsibilities within an organization. From an application portal view, it can be assigned to a user and can be transferred to or shared between multiple users. The basic principles in creating the roles are that a role must be transferable between users, assigned to more than one user and also revoked.

B. Assigning permissions to each role. Permissions refer to the operations that can be performed on information. Presuming that each role is a reflection of an information category, specific permissions are determined by the information itself.

C. Creating a group of users for each role. This will allow an easier identification of relation between information categories and access control groups. Is a good practice to create groups with several levels of parent-child kind, according to similarities between roles, this ensuring a stable propagation of roles and therefore of permissions. From a portal access perspective, a level of groups is basically a customised grouping of groups. In portal applications the level of groups is the criteria that a user must satisfy in order to access specific functionalities.

D. Assigning users to groups. This will determine which users may and which may not operate on the initial determined information categories.

3. ACL-based model implementation example

As an exemplification of ACL model implementation, we consider referring to some of the information regarding companies, information highly used in management. The information stored are related to name, vat number, legal form, address, phone numbers and fax numbers, email addresses, websites, activity code, activity description.

Following the steps presented above for ACL model implementation, the first step is to categorize the information and creating the roles. The identified categories and the corresponding roles created are:

- Identification, referring to name, vat number and legal form;
- Contact, referring to address, phone and fax numbers, emails and websites addresses;
- Activity, referring to activity code and description.

Assigning permissions to roles can be determined as follows:

- Identification: a company can be viewed, inserted, its name and vat number updated and also deleted, so the permissions are: view, insert, update and delete
- Contact: contact information can be viewed, inserted, updated and deleted with the same permissions
- Activity: as similar to identification and data, this information can be also viewed, inserted, updated and deleted.

One must note that the above permissions are only coincidentally the same for all roles.

The next step is creating user groups for each role and, if applicable, level groups. Created user groups are presented in figure 2. As seen on Figure 2, a group of groups named "*Data*" has been created in order to represent the possibilities of grouping information based on similarities. The levelling of groups allows a better separation of roles.

Therefore, for example, a user with access on level 3 will not be able be interfere with above level groups (*Identification* and *Data*). Furthermore, a user part of *Activity* group on level 3 cannot interfere neither with above level groups nor *Contact* group at the same level. But a user part of *Company* group at level 1 will have access to all information stored in below level groups.

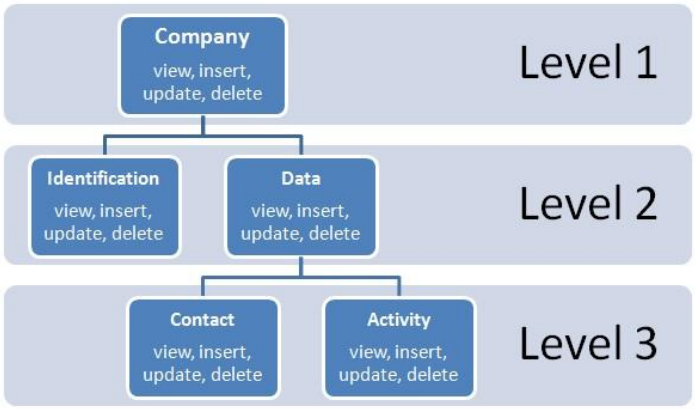

Figure 2. Group levels, user groups and permissions.

Assigning the users to groups is done taking into consideration the information they must access or not in order to fulfil their tasks.

4. Conclusions

The ACL model presented above is a relatively simple to implement solution to gain access control to information once the mentioned steps are steps are completed and correctly filled in.

Bibliography

[1] http://en.wikipedia.org/wiki/Computer_security_model
[2] http://en.wikipedia.org/wiki/Security_policy
[3] http://en.wikipedia.org/wiki/Access_control_list
[4] http://en.wikipedia.org/wiki/Intranet_portal
[5] http://magazine.joomla.org/issues/issue-aug-2012/item/825-A-Case-for-Role-Based-ACL

ACKNOWLEDGEMENT: This paper is supported by the Sectoral Operational Programme Human Resources Development (SOP HRD), ID137516 financed from the European Social Fund and by the Romanian Government.