

**METHOD AND SYSTEM FOR ADVANCED
ROLE-BASED ACCESS CONTROL IN
DISTRIBUTED AND CENTRALIZED
COMPUTER SYSTEMS**

FIELD OF THE INVENTION

The present invention relates to the technical field of role-based access control methods and security systems in distributed and centralized computer systems. More specifically, the invention relates to a method for controlling access rights of subjects on objects in a computer system by controlling said access rights dependent on a membership of a subject to a role. Furthermore, the invention relates to a system for registration, authorization, and control of access rights of subjects on objects in a computer system, wherein the system comprises users, groups, and access control lists at each object providing the access rights on the respective object.

DESCRIPTION OF THE PRIOR ART

In a computer system the accesses of users to data have to be controlled for security needs of the enterprise or organization using this computer system. The control of these accesses is performed by using access rights defining whether and how a user may access data in the computer system. This access control is performed by a security system which is integrated in or added to the operating system of the computer system. This security system performs a specific method for controlling access rights.

In most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator. All access rights of all users on an object form an access control list (ACL) associated to the object. When an access request occurs during operation time of the computer system from a user or, more generally, from a subject to the object, then the security system looks at the access control list of the respective object and decides whether the subject may access the object in the requested manner. These broadly installed security systems allow a so-called "per-object-review" of access rights, that is, to determine the kind of access rights of all subjects of a computer system to a respective object.

Since it is very inconvenient for a system administrator to provide each user with individual access rights, and to achieve a higher grade of data security and integrity in a computer system, a Role-Based Access Control (RBAC) method has been developed. Therein, a role is mainly a definition of a job at the lowest level of granularity used in the enterprise or organization. In a role-based access control system the system administrator only has to grant or revoke access rights to a role and has to group different subjects under each role.

In F. H. Lochovsky: "Role-Based Security in Data Base Management Systems" which is incorporated in C. E. Landwehr (editor): "Database Security: Status and Prospects", Elsevier Science Publishers B. V., 1988, pp. 209-222, the use of roles and objects in specifying a security mechanism for data base management systems is discussed. Using the idea that a user can play certain roles, authorization is specified using these roles.

In R. W. Baldwin: "Naming and Grouping Privileges to Simplify Security Management in Large Data Bases", Proceedings of IEEE Symposium on Security and Privacy, Oakland, 1990, pp. 116-132, authorization and control of

access rights in large security systems in the field of data base objects are described.

In D. Ferraiolo et al: "Role-Based Access Controls", Proceedings of the 5th National Computer Security Conference, October 1992, pp. 554-563, the role-based access control method is described in detail. Access control decisions are often based on the roles individual users take on as part of an organization. A role specifies a set of transactions that a user or set of users can perform within the context of an organization. Role-based access control provides a means of naming and describing relationships between individuals and access rights, providing a method of meeting the secure processing needs of many commercial and civilian government organizations.

Concerning the method of controlling access rights in a computer system as known from the existing role-based access control methods it is disadvantageous that a large number of similar but not identical job positions in an organization requires a large number of roles. This large number of roles causes a high storage requirement for the security system within the computer system. Furthermore, it is disadvantageous that the large number of roles causes high computing requirements for the security system. Both aspects lead to high costs for the operation of the security system. Furthermore, it is disadvantageous that the large number of roles makes it very difficult to manage the security system. The system administrator has to create a new role when a person remains in his job position but changes his location or project. This will cause higher costs or even less system security. Furthermore, since a role includes the union of all accesses and objects which users of that role have in different organization units of the enterprise. This means that the role will not necessarily contain the least privileges necessary for the functions of that role, i.e., a violation of the "Least Privilege Principle". However, if one attempts to mitigate the lack of access granularity with defining different roles based on access and object contexts, which may be possible in some designs, an administrative mechanism becomes necessary to relate these roles so that their consistent administration, e.g., update, becomes possible. Such a mechanism is not available today.

Concerning the access control system, it is disadvantageous that the existing role-based access control systems do not use the existing security mechanisms of the installed computer systems based on the existence of access control lists. Therefore, new security mechanisms or even a new security systems have to be implemented on the existing computer system. This causes additional hardware and software development with related high costs. This is even more disadvantageous in distributed or large centralized computer systems. Existing standard access control mechanisms for distributed systems as described in "Introduction to OSF DCE", Open Software Foundation (OSF), 1991, allow scalability to very large distributed systems. To date no role-based access control method scalable to large distributed systems exists.

It is an object of the present invention to provide a method for controlling access rights that is scalable to very large distributed computer systems and requires less storage and computing performance for the security system. Furthermore, it is an object of the invention to provide a role-based method for controlling access rights that does not necessarily violate the "Least Privilege Principle" but at the same time is more flexible and more convenient for the system administration.

Concerning the system for authorization and control of access rights, it is an object of the invention to provide a