

# IMPLEMENTATION OF ROLE-BASED ACCESS CONTROL IN MULTI-LEVEL SECURE SYSTEMS

## CROSS-REFERENCE TO RELATES APPLICATION

This application claims priority from Provisional Patent Application Ser. No. 60/032,531, filed Dec. 6, 1996.

## FIELD OF THE INVENTION

The present invention relates to security in computer systems. More particularly, the invention relates to control of the access of users to objects protected by known lattice-based multi-level secure systems.

## BACKGROUND OF THE INVENTION

### 1. Multi-level Secure (MLS) Systems

Traditionally, managing the security of a computer system has required mapping an organization's security policy to a relatively low-level set of controls, typically access control lists. That is, assuming individual persons are first identified to the system in a satisfactory manner, their access to documents, programs, facilities, and other "objects" within the protected computer system is then controlled by a security system simply by comparing the user's name against a list of names of persons entitled to access the given object.

According to a more sophisticated and very well-developed model for security of computer systems used widely throughout the U.S. military, and elsewhere, access to objects in a computer system is controlled by a "multi-level secure" ("MLS") system. A very significant investment has been made in development, verification, and implementation of such MLS systems. The present invention relates to a more convenient method of use of existing MLS systems than is now provided, but does not vitiate any of the security features provided by existing MLS systems; instead, the improvement provided by the present invention operates in conjunction with existing MLS systems. Accordingly, implementation of the present invention does not involve devaluation or modification of existing MLS systems, which would be very undesirable; not only would this be very costly, but the known security of existing MLS systems would no longer be available.

Existing MLS systems are referred to as "lattice-based" because objects to which access is controlled thereby may be thought of as located on a two-dimensional lattice, in which one dimension is a security level, such as SECRET, TOP SECRET, etc., and the other dimension is a grouping by subject matter or the like. See FIG. 1, depicting a schematic representation of an MLS lattice. Here, the vertical axis represents various levels 10 of security, while the horizontal axis represents objects 14 protected by the system, organized by categories 12. The categories may be subject-matter-related, e.g., Procurement, Personnel, or Public Relations, or may be organized by further security classifications, e.g., NATO, NOFORN (an acronym for "No Foreign Nationals"), or the like.

According to MLS, all objects are assigned one or more "compartments", which are simply labels used to index the objects. Access to the objects is then provided by giving the requester access to compartments including those of the objects requested and of a equal or lesser security level. Again assuming individual persons are first identified to the system in a satisfactory manner, a subject (again, an

individual, another computer system, or the like) seeking access to an object (a document, a control path, a communication path, or the like) protected by the system must thus have been assigned access to the compartment within which the object is located and must possess a security clearance at least equal to that of the object. See generally, "Role-Based Access Controls", Ferraiolo et al, *Proceedings of the 15th NIST-NSA National Computer Security Conference*, 1992.

As a practical matter, implementation of the the MLS "kernel" as above requires that each user must be separately assigned numerous "privileges", i.e., the right to access certain objects or groups of objects within the system. In a large MLS system, with hundreds or thousands of users, and as many objects, maintenance of the proper "connections", that is, assignment of privileges with respect to various objects to individual users, is a substantial administrative burden. Particularly when an individual changes job assignments, all connections between that individual and objects to which he or she previously had access must be severed, and new connections must be established to all objects needed for performance of the new function.

As mentioned, however, there has been a very substantial investment made in MLS systems to date; they are tested, verified, and trusted, and so any new system attempting to simplify the use of MLS systems must as a first criterion not vitiate the security provided thereby.

### 2. Role-Based Access Control

Briefly stated, in role-based access control (RBAC) systems, access to an object within a computer system is provided to the members of groups termed "roles"; all subjects belonging to a given role have the same privileges to access various objects within the system. Individuals are then granted access to objects by being assigned membership in appropriate roles.

RBAC is considered useful in many commercial environments because it allows access to the computer system to be conveniently organized along lines corresponding to the actual duties and responsibilities of individuals within organizations. For example, RBAC allows the access provided by roles to conform to a preexisting hierarchy; in a hospital environment, members of the "doctor" role will have broader access to protected objects than would members of "nurse", who will in turn be given broader access than "health-care provider". Various types of privilege can be conveniently organized as a function of role assignments. For example, "doctor" membership may allow the user the privilege to read from or write to a pharmacy record, while "pharmacist" may only allow reading therefrom. Cardinality may be enforced; that is, only one general manager may exist at a given time. Roles may be exclusive; that is, an individual who is a member of "trader" in a commercial bank could not also be a member of "auditor" at the same time.

A particular advantage of RBAC is that it allows the access privileges provided to individuals to be very conveniently reconfigured as the individuals change job requirements, simply by deleting one's original assignment to a first role and adding one to the new role.

RBAC is described in Ferraiolo et al (1992), *supra*, and operational RBAC software is available from several vendors.

A rigorous mathematical basis for RBAC is provided by the inventor and others in Ferraiolo et al, "Role based access control: Features and motivations", *Annual Computer Security Applications Conference*, IEEE Computer Society Press, 1995. This paper, which is not prior art to the present