Home

Role Engineering & RBAC Standards

RBAC & Sarbanes-Oxley Compliance

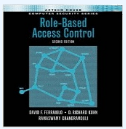
RBAC Case Studies

NIST RBAC Patents

Helpful RBAC Resources

Contacts

Frequently Asked Questions (FAQs)

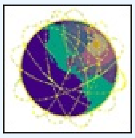


RBAC book

"A must read."
Review from IEEE Computer Society, Security & Privacy
"Overall, this is a great book."
Linux Journal

2002 Gold Medal for Scientific/ Engineering Achievement - US Department

1998 Excellence in Technology Transfer Award - Federal Laboratory Consortium



1998 Best Paper - Nat Inf Systems Security Conf

AN INTRODUCTION TO ROLE-BASED ACCESS CONTROL

NIST/ITL Bulletin, December, 1995

This bulletin provides background information on Role-Based Access Control (RBAC), a technical means for controlling access to computer resources. While still largely in the demonstration and prototype stages of development, RBAC appears to be a promising method for controlling what information computer users can utilize, the programs that they can run, and the modifications that they can make. Only a few off-the-shelf systems that implement RBAC are commercially available; however, organizations may want to start investigating RBAC for future application in their multi-user systems. RBAC is appropriate for consideration in systems that process unclassified but sensitive information, as well as those that process classified information.

What Is Role-Based Access Control?

Access is the ability to do something with a computer resource (e.g., use, change, or view). Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls). Computer- based access controls can prescribe not only who or what process may have access to a specific system resource, but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices.

With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.

Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies.

The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process.

Users And Roles

Under the RBAC framework, users are granted membership into roles based on their competencies and responsibilities in the organization. The operations that a user is permitted to perform

Background on access control: DAC, MAC, and RBAC

Access control technology has evolved from research and development efforts supported by the Department of Defense (DoD). This research has resulted in two fundamental types of access control: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). While initial research and applications addressed preventing the unauthorized access to classified information, recent applications have applied these policies to commercial processing environments.

DAC permits the granting and revoking of access control privileges to be left to the discretion of the individual users. A DAC mechanism allows users to grant or revoke access to any of the objects under their control. As such, users are said to be the owners of the objects under their control. However, for many organizations, the end users do not own the information for which they are allowed access. For these organizations, the corporation or agency is the actual owner of system objects as well as the programs that process them. Access priorities are controlled by the organization and are often based on employee functions rather than data ownership.

MAC, as defined in the DoD's Trusted Computer Security Evaluation Criteria (TCSEC), is "A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e.

are based on the user's role. User membership into roles can be revoked easily and new memberships established as job assignments dictate. Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve. This simplifies the administration and management of privileges; roles can be updated without updating the privileges for every user on an individual basis.

When a user is associated with a role: the user can be given no more privilege than is necessary to perform the job. This concept of least privilege requires identifying the user's job functions, determining the minimum set of privileges required to perform that function, and restricting the user to a domain with those privileges and nothing more. In less precisely controlled systems, this is often difficult or costly to achieve. Someone assigned to a job category may be allowed more privileges than needed because is difficult to tailor access based on various attributes or constraints. Since many of the responsibilities overlap between job categories, maximum privilege for each job category could cause unlawful access.

clearance) of subjects to access information of such sensitivity."

These policies for access control are not particularly well suited to the requirements of government and industry organizations that process unclassified but sensitive information. In these environments, security objectives often support higher-level organizational policies which are derived from existing laws, ethics, regulations, or generally accepted practices. Such environments usually require the ability to control actions of individuals beyond just an individual's ability to access information according to how that information is labeled based on its sensitivity.

Roles And Role Hierarchies

Under RBAC, roles can have overlapping responsibilities and privileges; that is, users belonging to different roles may need to perform common operations. Some general operations may be performed by all employees. In this situation, it would be inefficient and administratively cumbersome to specify repeatedly these general operations for each role that gets created. Role hierarchies can be established to provide for the natural structure of an enterprise. A role hierarchy defines roles that have unique attributes and that may contain other roles; that is, one role may implicitly include the operations that are associated with another role.

In the healthcare situation, a role Specialist could contain the roles of Doctor and Intern. This means that members of the role Specialist are implicitly associated with the operations associated with the roles Doctor and Intern without the administrator having to explicitly list the Doctor and Intern operations. Moreover, the roles Cardiologist and Rheumatologist could each contain the Specialist role.

Role hierarchies are a natural way of organizing roles to reflect authority, responsibility, and competency:

the role in which the user is gaining membership is not mutually exclusive with another role for which the user already possesses membership. These operations and roles can be subject to organizational policies or constraints. When operations overlap, hierarchies of roles can be established. Instead of instituting costly auditing to monitor access, organizations can put constraints on access through RBAC. For example, it may seem sufficient to allow physicians to have access to all patient data records if their access is monitored carefully. With RBAC, constraints can be placed on physician access so that only those records that are associated with a particular physician can be accessed.

Roles And Operations

Organizations can establish the rules for the association of operations with roles. For example, a healthcare provider may decide that the role of clinician must be constrained to post only the results of certain tests but not to distribute them where routing and human errors could violate a patient's right to privacy. Operations can also be specified in a manner that can be used in the demonstration and enforcement of laws or regulations. For example, a pharmacist can be provided with operations to dispense, but not to prescribe, medication.

An operation represents a unit of control that can be referenced by an individual role, subject to regulatory constraints within the RBAC framework. An operation can be used to capture complex security-relevant details or constraints that cannot be determined by a simple mode of access.

For example, there are differences between the access needs of a teller and an accounting supervisor in a bank. An enterprise defines a teller role as being able to perform a savings deposit operation. This requires read and write access to specific fields within a savings file. An enterprise may also define an accounting supervisor role that is allowed to perform correction operations. These operations require read and write access to the same fields of a savings file as the teller. However, the accounting supervisor may not be allowed to initiate deposits or withdrawals but only perform corrections after the fact. Likewise, the teller is not allowed to perform any corrections once the transaction has been completed. The difference between these two roles is the operations that are executed by the different roles and the values that are written to the transaction log file.

The RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances:

only those operations that need to be performed by members of a role are granted to the role. Granting of user membership to roles can be limited. Some roles can only be occupied by a certain number of employees at any given period of time. The role of manager, for example, can be granted to only one employee at a time. Although an employee other than the manager may act in that role, only one person may assume the responsibilities of a manager at any given time. A user can become a new member of a role as long as the number of members allowed for the role is not exceeded.

Advantages Of RBAC

A properly-administered RBAC system enables users to carry out a broad range of authorized operations, and provides great flexibility and breadth of application. System administrators can control access at a level of abstraction that is natural to the way that enterprises typically conduct business. This is achieved by statically and dynamically regulating users' actions through the establishment and definition of roles, role hierarchies, relationships, and constraints. Thus, once an RBAC framework is established for an organization, the principal administrative actions are the granting and revoking of users into and out of roles. This is in contrast to the more conventional and less intuitive process of attempting to administer lower-level access control mechanisms directly (e.g., access control lists [ACLs], capabilities, or type enforcement entities) on an object-by-object basis.

Further, it is possible to associate the concept of an RBAC operation with the concept of "method" in Object Technology. This association leads to approaches where Object Technology can be used in applications and operating systems to implement an RBAC operation.

For distributed systems, RBAC administrator responsibilities can be divided among central and local protection domains; that is, central protection policies can be defined at an enterprise level while leaving protection issues that are of local concern at the organizational unit level. For example, within a distributed healthcare system, operations that are associated with healthcare providers may be centrally specified and pertain to all hospitals and clinics, but the granting and revoking of memberships into specific roles may be specified by administrators at local sites.

Status Of Current RBAC Activities

Several organizations are experimenting with the inclusion of provisions for RBAC in open consensus specifications. RBAC is an integral part of the security models for Secure European System for Applications in a Multi-vendor Environment (SESAME) distributed system and the database language SQL3. In addition, the Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA) Security specification uses RBAC as an example of an access control mechanism which can be used with the distributed Object Technology defined by the OMG. (See reference below.)

CSL has been developing and defining RBAC and its applicability cooperatively with industry, government, and academic partners. In conjunction with Dr. Ravi Sandhu of George Mason University and Seta Corporation, CSL is defining RBAC and its feasibility. We are working with Dr. Virgil Gligor and his associates at the University of Maryland and with the National Security Agency (NSA) to develop a formal reference model for RBAC to provide a safe, effective, and consistent mechanism for access control. This effort is also implementing RBAC on NSA's Synergy Platform, a secure platform based on the Mach Operating System. CSL is also developing a demonstration of RBAC use in healthcare. The access policy used in this demonstration is based on a draft consensus policy for patient record access developed in the United Kingdom. In conjunction with the Internal Revenue Service (IRS), CSL is defining roles and operations suitable for the IRS environment. In conjunction with the Veterans Administration (VA), CSL is studying the applicability of

RBAC to VA systems.

Based on current research and experience, RBAC appears to fit well into the widely varying security policies of industry and government organizations.

For additional information on Role-Based Access Control see:

http://csrc.nist.gov/rbac/

or contact
David Ferraiolo, dferraiolo@nist.gov, 301-975-3046
Rick Kuhn, kuhn@nist.gov, 301-975-3337

References

Department of Defense, "Trusted Computer Security Evaluation Criteria," DoD 5200.28-STD, 1985.

David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls," Proceedings of the 15th NIST-NSA National Computer Security Conference, Baltimore, Maryland, October 13-16, 1992.

David F. Ferraiolo, Dennis M. Gilbert, and Nickilyn Lynch, "An Examination of Federal and Commercial Access Control Policy Needs," Proceedings of the 16th NIST-NSA National Computer Security Conference, Baltimore, Maryland, September 20-23, 1993.

ISO/IEC 9075, (Working Draft) Database Language SQL - Part 2: Foundation, Document ISO/IEC JTC1/SC21 N9463, March 1995.

A. Griew and R. Currell, "A Strategy for Security of the Electronic Patient Record," Institute for Health Informatics, Aberystwyth, Draft Version 2.1, March 8, 1995.

David F. Ferraiolo, Janet A. Cugini, and D. Richard Kuhn, "Role-Based Access Control (RBAC): Features and Motivations," 11th Annual Computer Security Applications Proceedings, 1995.

John Barkley, "Application Engineering in Health Care," Proceedings of the 2nd Annual CHIN Summit, 1995.

CORBA Security Draft, Object Management Group (OMG) Document Number 95-9-1, September 1995.

John Barkley, "Implementing Role-Based Access Control using Object Technology," First ACM Workshop on Role-Based Access Control, Gaithersburg, Maryland, November 30-December 1, 1995.

T. Parker and D. Pinkas, "SESAME Technology Version 3: Overview,"

http://www.esat.kuleuven.ac.be/cosic/sesame/doc-txt/overview.txt