

Y-12

**Oak Ridge
Y-12
Plant**

**CONTROLLING NEED-TO-KNOW ACCESS
USING RULE BASED ALGORITHMS**

J. D. McClanahan
Data Systems Research and Development Division

C. H. Malarkey
Data Systems Research and Development Division

May 6-7, 1998

Preprint for submission to:
Inforum '98
Oak Ridge, Tennessee
May 6-7, 1998

Prepared by the
Oak Ridge Y-12 Plant
Oak Ridge, Tennessee 37831
managed by
Lockheed Martin Energy Systems, Inc.
For the
U.S. DEPARTMENT OF ENERGY
Under contract DE-AC05-84OR21400

CONTROLLING NEED-TO-KNOW ACCESS USING RULE BASED ALGORITHMS

I. INTRODUCTION

In today's highly integrated computing environments, it is imperative that access to data objects be controlled based on the need-to-know (NTK) of the requester. As Web-based applications and high-speed communication lines make it easier and faster to find, transfer, and view digitized documents and drawings we have to move away from traditional access algorithms toward those which can ensure that the person requesting an object is authorized to access the document. Traditional access algorithms have assumed a common need-to-know for all users sharing a local area network (LAN) or for all users who have logon accounts and authorization to use specific applications. In the future applications should provide mechanisms to determine need-to-know access based on rules established for a user's profile and a data object's content.

This presentation will discuss the importance of authorizing access determined from the content of the document. It will demonstrate the formation of access rules, which capture the user's need-to-know, and how the user's profile is matched with the document content to ensure authorized access.

Examples presented of rule based need-to-know definition and control will be based on the Electronic Document Management System (EDMS) at the Y-12 plant. This application has managed content-based NTK and access control within the LMES product definition environment since 1987.

II. NEED-TO-KNOW REQUIREMENTS

Need-to-know requirements have been implemented for as long as information has been generated and communicated between individuals. Typical business drivers for protecting data include issues of national security, proprietary data that is patented or copyrighted, and sensitive data that is managed according to privacy act legislation. Organizations are required to ensure that only authorized individuals with an established need-to-know have access to the company's critical intellectual property. Need-to-know is frequently viewed from the standpoint to the requester's job responsibility within the organization.

When everything was managed and communicated by paper, the creator was able to maintain a level of control over the distribution and dissemination of the paper copy. For the initial distribution of a document, need-to-know was usually accomplished by ensuring that those on the distribution list were authorized to receive and use the information contained within the document. Any secondary distribution of the paper copy of a document by the original recipients was also assumed to be consistent with informal, unofficial need-to-know requirements.

The computing environment has brought about changes in the perceptions of how to protect electronic data and in how to establish and manage need-to-know.

III. TRADITIONAL ACCESS CONTROL

Access control is managed at several levels within the electronic environment. When information is to be shared, it must be moved from the creators stand-alone PC or workstation to a location where others can retrieve it. Traditionally, these shared areas are established on mainframes or servers to which a user applies for an account. In the process of establishing accounts, users are provided with unique identification and passwords. Since all operating systems environments manage access through logon accounts and passwords, this is the first level of managing access control.

A second level of controlling access is managing authorization to directory structures and application execution. Once an account is established, the user must be authorized to execute the software application that manages the data. Application views are defined which provide information used by the computer's operating system and an application's database to determine a user's role at run-time. Usually these application views are based on a specific user function such as product engineering or software application management. The views also define the nature of the user's role in the software system. For example, one view is established for READ-ONLY access while another view will allow CREATE, READ, UPDATE, and DELETE of the data managed by the application. These application views are described in terms of a unique process identifier, which indicates the user's role. For example, the YIS_SXR_USER is a process identifier for a user of the Specification eXception Request (SXR) software system at Y-12. When a user is granted access to a particular software system, the correct process identifier is associated with the logon account. Users may have as many process identifiers as they need to accomplish their job assignments. A user's application access is formally requested by his or her management and is approved by the individual who is the documented view administrator. Usually, the view administrator is the data sponsor or someone who has been designated by the data sponsor as responsible for granting access to the data. Each access request is only authorized for a one-year time period after which the access authorization must be reviewed by the view administrator and re-approved.

The process identifier is applied to the directory structure, the database structure, and the application's executable image as a method of matching the user's authorized access to the type of access defined for the software system. These levels of access control ensure that the user's access to certain classes of information is authorized, they do not provide the final level of access control necessary to ensure need-to-know. Controlling access based on document content and a user's profile satisfies this last level of authorization.

IV. RULE BASED ALGORITHMS

Designers of applications and data owners must consider the types of NTK that apply to the data maintained by the software application. In the suite of applications that comprise the EDMS software, the users' job responsibility is a major factor in their NTK access. For example, two of the primary software users are product engineers and quality engineers. Both groups usually

have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as weapon programs and manufacturing areas.

In order to manage NTK, application specific position codes and access profile rules are maintained for each user. When storing the data object, the data owner identifies attributes that describe the document's content and purpose. At the time of application execution, the user position codes and user's profiles are matched with document attributes to determine NTK.

V. USER PROFILES

Position codes are stored in internal tables to control access, especially to specific functions within the application. The position code table contains the user's badge number (which is the unique method of identifying employees and subcontractors within the application), the application to which the position code applies, and the position code itself.

| POSITION-CODE |
|--|
| EMP-BN X(6) APPLICATION-ID X(4) EMP-POSITION-CODE X(2) |

An employee may have multiple rules active at any point in time. In addition, any rule may be activated or deactivated depending on circumstances identified by the employee's management. An additional feature captured in conjunction with the employee's access rule is a notification indicator. This flag determines whether or not the individual is notified when a revision in the document to which the rule applies is distributed.

| EMP-ACCESS-RULE | |
|--|--|
| EMP-BN X(6) EMP-ACCESS-RULE-NO (SW) | EMP-ACCESS-NOTIF-CODE X(1) EMP-ACCESS-RULE-ENABLE-FLAG X(1) |

Each rule may identify multiple attributes to be matched with required values and attributes related to instances of the document. An attribute is a method by which the content of the document is described. When an attribute value is specified in association with an employee's access rule, it provides the NTK profile which must be matched in order to allow access to the instance of a document.

| EMP-ACCESS-ATTRIBUTE |
|--|
| EMP-BN X(6) EMP-ACCESS-RULE-NO (SW) EMP-ACCESS-RULE-ATTRIBUTE-CODE X(5) EMP-ACCESS-RULE-ATTRIBUTE-VAL X(20) |

At the document revision level, there are additional required elements for storage. Those that are specified for access control include the classification and the information that identifies the operating unit and division associated with the data object.

| DOC-REV | |
|-----------------------------------|--|
| DOC-NO X(18) DOC-REV-CODE X(6) | DOC-CLASS-LEVEL-CODE X(4) DOC-CLASS-CAT-CODE X(5) . . . OPER-UNIT-RESP-FOR-DOC-NO X(1) DIV-RESP-FOR DOC-NO X(3) . . . |

An occurrence of a document may have multiple attributes associated with it and certain attributes are required for some categories of documents. In the case of product definition documents at least one program and manufacturing center must be specified.

| DOC-ATTRIBUTE |
|---|
| DOC-NO X(18) DOC-REV-CODE X(6) EMP-ACCESS-RULE-ATTRIBUTE-CODE X(5) EMP-ACCESS-RULE-ATTRIBUTE-VAL X(20) |

Attribute codes vary based on the category and type of document. For example, product definition documents identify values for attribute codes that include program, responsibility area (i.e., manufacturing center), process number, product identifier, work request number, building, machine, part number.

VII. DIVISION PROFILE MANAGER ROLE

There are two application management functions that are critical to the identification and maintenance of information used for access control. One is the role of division profile manager and the other is the software application manager.

The division profile manager is responsible for the creation of user position codes and profiles for those employees who report to him or her. It is through this function that a manager provides the ability to automate the NTK for electronic data using rule-based algorithms.

Usually there is only one or two software application managers (SAM) per system. The SAM is responsible for the creation of the predefined document categories and types, for definition and identification of attribute codes, and for the specification of position codes. All reference and validation

tables used by the software systems are provided through this role that is held by a person from the business community.

VIII. RUN TIME ACCESS

During program execution, the application controls processing and read-write access to data based on the process identifiers, the position codes, and the NTK parameter controls. When data is being retrieved through queries for read-only purposes such as viewing and printing, access rules are not checked. However, only the non-classified data elements of document number, revision code, and an unclassified title are displayed to the user as results from a query. Access authorization is verified when the user selects a specific a document from the retrieved list. If the user's NTK profile matches the documents access parameters, the application proceeds with the display. However, if the user is not authorized for access, an access request failure is logged.

IX. ACCESS LOGS

Multiple log entries are kept by the EDMS system including several types of access logs. Among some of the access entries are those where a non-authorized user attempts to run an application or to gain access through some other unauthorized means. Access failures as well as retrievals using NTK rules are logged. Although the SAM can review these logs at any time, a yearly report is generated and monitored by the SAM who distributes it to line management for review. The division profile managers use the annual report to determine that user profiles are accurate and to verify that the user and the application are handling NTK rules correctly.

X. SUMMARY

Establishing what NTK is and how to apply it across today's automated, highly integrated environments is a significant challenge. Data owners must feel confident that their information is secure and protected and that it is only disseminated to those who are authorized to access it.

The EDMS application has been in production since 1987. At the time of production implementation the NTK algorithms were certified by the Computer Security Organization (CTSO) and by Y-12 and DOE Information Security officers. One of the advantages of the rule based access control implemented within the application has been that user authentication was consistent with requirements for ensuring a secure environment. The system was authorized to track document classification, comments, and approvals electronically prior to the advent of digital signatures.

BIOGRAPHY:

NAME: Jim McClanahan

ORGANIZATION: Lockheed Martin Energy Systems – Data Systems Research and Development

PO Box 2009 MS 8160

Oak Ridge, Tn 37831-8160

Phone: (423) 574-2948

Fax: (423) 574-4748

E-mail: jdv@ornl.gov

Jim McClanahan is a Computer Analyst that has been working with Electronic Document Management Systems (EDMS) for the last ten years. He has been working with an in-house based EDMS that manages access to documents and drawings up to Secret-Restricted Data at the Y-12 plant in Oak Ridge. Jim received his Bachelor's of Science degree in Computer Science from Tennessee Technological University in 1986.

DISTRIBUTION

1. C. H. Malarkey, 9103, MS-8160
2. J. D. McClanahan, 9103, MS-8160
3. P. H. Prewett, 9113, MS-8208
4. R. E. Textor, 9103, MS-8142
5. Y-12 Central Files, 9711-5, MS-8169