



Inside this issue:

- ✍ **Abstract Review**
- ✍ **Healthcare Scenario Roadmap – HL7 Update**
- ✍ **Health Level Seven (HL7) Security and Accountability Technical Committee – DSTU Ballot Update**
- ✍ **Upcoming Meetings**

VHA/IHS RBAC TF Chair

Robert O'Hara, MD
Robert.Ohara@med.va.gov

VHA Deputy Chief Architect,

RBAC Project Manager
Steve Wagner
Steve.Wagner@med.va.gov

VHA Security Architect,

RBAC Architect
Mike Davis, CISSP
Mike.Davis@med.va.gov

VHA Security Architect,

RBAC Architect
Ed Coyne, PhD
Ed.Coyne@med.va.gov

VHA Software Security Architect

Amy Page
Amy.Page@med.va.gov

RBAC Project Lead

Suzanne Webb
Suzanne.Gonzales-Webb@saic.com

~

Abstract Review: A Framework for Multiple Authorization Types in a Healthcare Application System

Ramaswamy Chandramouli of the Computer Security Division of ITL has written a healthcare enterprise framework description for an Admission, Discharge and Transfer System (ADT). The following is a review of that paper.

The DAFMAT (Dynamic Authorization Framework for Multiple Authorization Types) framework uses a combination of Role-Based Access Control (RBAC) and Dynamic Type Enforcement (DTE) augmented with a logic-driven authorization engine. The application of DAFMAT for evaluation and determining various types of authorization requests for the Admissions, Discharge and Transfer System (ADT) in a healthcare enterprise was described.

The need to support sophisticated authorization policies has grown tremendously in the last few years for many vertical market applications. For example, healthcare application systems dealing with patient-identifiable information will shortly be required to comply with requirements in the HIPAA (Health Insurance Portability and Accountability Act) Security Standards [1]. These standards, as written by R. Chandramouli, stipulate that healthcare application systems should have features for user-based, role-based and context-based authorizations as well as capabilities for making emergency authorizations.

In most of the current authorization frameworks in application systems, the authorization for a user operation is determined using a static database like ACL entries or system tables. These frameworks cannot provide the foundation for supporting multiple types of authorizations like emergency authorizations, context-based authorizations etc, as required by HIPAA security standards. An authorization framework that can provide this critical functionality is proposed in this paper. The framework is based on a combination of Role-Based Access Control (RBAC) and Domain Type Enforcement (DTE) access control models augmented with a logic-driven authorization engine. We have used the acronym DAFMAT (Dynamic Authorization Framework for Multiple Authorization Types) to refer to this framework.

The application of DAFMAT to derive various types of authorizations for an important class of healthcare application system called the Admissions, Discharge and Transfer System (ADT) is also illustrated in this paper.

Underlying Concepts in DAFMAT Framework

RBAC is a higher-level access control model that uses the abstraction concept of roles to reduce the complexity of an authorization management scheme [2]. The most important constructs are users, roles and permissions and the relations involving these constructs. In RBAC, users are assigned to roles, and permissions are assigned to roles. Users derive all their permissions by virtue of their role memberships. A single user can be assigned to multiple roles and a single role can be assigned to multiple



UPCOMING MEETINGS

- ✉ **HL7 January 2006 Working Group Meeting**
January 8-13, 2006
Phoenix, Arizona
- ✉ **INCITS CS1 Task Group, Cyber Security**
February 1-2, 2006
San Jose, California
- ✉ **HIMSS Annual Conference and Exhibition**
February 12-16, 2006
San Diego, California
- ✉ **NIST and FISSEA Conference – Training for a Cyber-Secure Future,**
March 20-21, 2006
Bethesda, Maryland
- ✉ **ASTM Committee E31 on Healthcare Informatics,**
May 22-24, 2006
Baltimore, Maryland

~

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121
Or e-mail:
Suzanne.Gonzales-Webb@va.gov

users. In addition, we can also define structures for organizing roles found within an enterprise (e.g., a hierarchical structure).

Comparison with Related Work

Combining RBAC with DTE was first illustrated by Hoffman [3]. Making use of the fact that RBAC provides good higher-level abstraction mechanisms for expressing different types of policies ([4], [5]) like the Principle of Least Privilege and Conflict of Interest etc., this work illustrated a way of implementing those policies using the control mechanisms of DTE on a secure operating system. However Hoffman's implementation is based on static associations between users, roles, subjects and domains and did not provide a mechanism for incorporating transient information since it is not relevant from an operating system perspective. Tidswell and Potter [6.] illustrated a method of dynamically changing the configuration of a DTE Model.

Role-Domain Mapping

A domain, as defined in this paper; represents a functional area within an enterprise. In a healthcare enterprise a person occupying a job position (which is represented by a role) rarely performs any tasks outside his/her general functional area as it involves legal and professional competency issues. Hence several roles may be associated with a domain, but a role always belongs to a unique domain. Therefore the role to domain mapping is a many-to-one mapping defined using the function name RoleDomain as:

RoleDomain(role) >>-> domain (Role_Domain(role, domain))

RBAC-DTE Model Data for ADT

The sample "RBAC-DTE Model Data" set given in R. Chandramouli's illustration consists of the following; 4 users, 4 roles, 4 subjects and 3 domains, and provides a nice scenario example using ADT processing functionality.

Conclusions and Scope for Future Work

Authorization mechanisms that support multiple authorization types can provide effective control of access to resources in many vertical market applications. The DAFMAT framework is a way to provide this critical functionality using a hybrid access control model and a logic-driven authorization engine that makes use of contextual information. The same authorization engine can be used for dynamic reconfiguration of Domain-Type access matrix entries as well as for dynamic User-Role and Subject-Role assignments. However the inclusion of these features may make the authorization engine difficult to build and result in performance penalties for the authorization mechanism. However, sophisticated authorization rules can be implemented (without significant degradation of system response times) through the use of a common security kernel that will mediate access to a family of application systems within a healthcare enterprise as has been done in the VA healthcare settings.



RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121
Or e-mail:
Suzanne.Gonzales-Webb@va.gov

The presence of a security kernel may make integration of COTS application systems into the IT resources of a healthcare enterprise an expensive operation. Since IT infrastructures in most healthcare enterprises are heterogeneous, the most preferred alternative is to build application-level controls for authorizations by making sure that appropriate access control models and mechanisms are used to capture the enterprise authorization policy requirements.

References

- [1] Security and Electronic Signature Standards; Proposed Rule. Federal Register, Vol 63, No. 155, August 12, 1998.
- [2] D. Ferraiolo, J. Cugini, and D.R. Kuhn. "Role Based Access Control (RBAC): Features and Motivations" Proc. 11th Annual Computer Security Applications Conference, December 1995.
- [3] J. Hoffman. "Implementing RBAC on a type enforced system" Proc. 13th Annual Computer Security Applications Conference, December 1997.
- [4] R.S. Sandhu, E.J. Coyne, H.L. Feinstein and C.E. Youman. "Role Based Access Control Models" IEEE Computer, vol 29, Num 2, February 1996, p38-47.
- [5] J.F. Barkley, A.V. Cincotta, D.F. Ferraiolo, S. Gavrila and D.R. Kuhn. "Role based access control for world wide web" <http://hissa.ncsl.nist.gov/rbac/rbacweb/paper.ps>, April 1997.
- [6] J. Tidswell and J. Potter "An Approach to Dynamic Domain and Type Enforcement" Microsoft Research Institute, Department of Computing, Macquarie University, NSW Australia.

This paper can be found at the following link:
http://csrc.nist.gov/rbac/rmouli_healthcare.pdf

THE HEALTHCARE SCENARIO ROADMAP

Non-Licensed Personnel - Update

Additional information has been added to the January ballot in addition to the previously submitted information accepted by the HL7 Security Technical Committee to provide a more robust and complete DSTU vocabulary. This additional information also provides the opportunity to prepare for an RBAC demonstration at the HIMSS (Healthcare Information and Management Systems Society) conference in January 2006.

The task force assigned to prepare and submit the non-licensed healthcare portion of the permission catalog has completed the 99 ASTM Non-Licensed Healthcare Roles and associated permissions. In addition, specific VHA roles were also added. The RBAC Permission Definition



~

RBAC Newsletter Editor

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121
Or e-mail:
Suzanne.Gonzales-Webb@va.gov

Subcommittee concluded their task with an external peer review which resulted in zero additional permissions and very little disagreement on role assignments. Input from both the task force and the external review results was derived from licensed and non-licensed healthcare personnel in the field.

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE

Draft Standard for Trial Use (DSTU) Upcoming Ballot

The following materials have been prepared and submitted to HL7 to be voted upon as a Draft Standard for Trial use in the January 2006 upcoming Ballot.

- ? HL7 RBAC Healthcare Permission Catalog v2.2
- ? HL7 Healthcare Scenario Roadmap v2.19
- ? HL7 RBAC Healthcare Scenarios v2.0
- ? HL7 RBAC Role Engineering Process v1.1
- ? HL7 RBAC Role Engineer Process Applied Example v1.1

RBAC is critically important to the security aspects of healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website.

~