



Inside this issue:

- Health Level Seven (HL7) Security and Accountability Technical Committee – Upcoming Ballot
- Security and Business Rules in Role-Based Access Control
- HEALTHCARE Scenario Permissions Catalog - Update

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE –

Draft Standard for Trial Use (DSTU) Upcoming Ballot

The following materials have been prepared and will be submitted to HL7 to be balloted as a Draft Standard for Trial use in January 2006. The documents were approved with no negative comments by the HL7 Security technical committee and will be submitted for the upcoming ballot as a Draft Standard for Trail Use (DSTU).

- 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

Please see the HEALTHCARE Scenario Permissions Catalog Update for more information.

SECURITY AND BUSINESS RULES in ROLE-BASED ACCESS CONTROL APPLICATIONS

Security Principals

RBAC policies are increasingly being considered part of the distributed security infrastructure for service-oriented architectures, Web and N-Tier applications. At the same time, application rules are remaining with the application. This new environment requires re-examination of the fundamental definitions of security and business rules.

Separating security and business rules is an important aspect of requirements analysis and will be essential in implementing role-based access control in service-oriented environments such as a hospital or financial institution. Clearly distinguishing security from business rules is a necessary first step in developing standard roles suitable for use in distributed enterprise identity and access management infrastructures.

For RBAC purposes, the separation of business and security rules can be specified by evaluation against basic principles in the three domains of security independence, state and privilege. This approach works well for both the security engineer and application development community.

Security Independence

Security shall be enforced independent of application business logic.

The corollary to this principle is that security functions shall not be used to satisfy non-security objectives in standard implementations.

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

VHA Software Security Architect
Cynthia Kramer
Cynthia.Kramer@med.va.gov

≈



RBAC Newsletter Editor

ATTN: Suzanne Webb

RBAC Project Lead

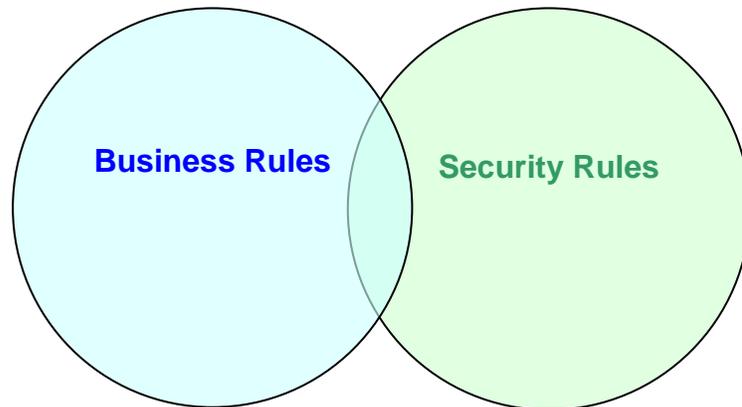
10260 Campus Point MS-B1E

La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@saic.com

Combined implementations tend to compromise the system security, lead to poor design, and do not support clear security roles. It has long been a tenant of security engineering to separate and isolate security and business application code. This separation is essential for security engineers to obtain a clear definition of security boundaries, ensure security code is not affected by changes to business logic, and support certification. Separation reduces the complexity and validity of unit, functional, and penetration testing at all phases of the product development life cycle. *—Excerpt taken from Security and Business Rules in Role-Based Access Control (RBAC) Applications document on the RBAC website.*



The figure above illustrates that business rules can also be security rules and vice-versa. RBAC will only create roles where the rule involves a requirement related to enforcing confidentiality, integrity or availability through security privilege.

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 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.



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.

