



Inside this issue:

- Health Level Seven (HL7) Security and Accountability Technical Committee
- INCITS Cyber Technical Committee Update
- HEALTHCARE Scenario Roadmap - Update
- XACML brief

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE – Working Group Meeting September 11-16, 2005 San Diego, California

The following materials prepared and submitted to the HL7 Security Technical Committee by VHA representatives for the August ballot cycle were approved with no negative comments:

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

The additional information being added to the January ballot, in addition to the above-submitted information, is scheduled to be completed by October 15, 2005 in preparation for a more complete DSTU. This date also provides the opportunity to prepare for an RBAC demonstration at the HIMSS conference in January 2006.

INCITS CYBER SECURITY (CS1) TECHNICAL COMMITTEE, SEPTEMBER 27-28, 2005, WASHINGTON, DC

RBAC proposal “Requirements for the Implementation of Role Based Access Control (RBAC)” was approved by the CSI Technical Committee. Authors were Rick Kuhn of NIST and VHA Security Architect, Mike Davis. The result will be a standard that addresses RBAC implementation requirements. This proposal was balloted at the September 2005 meeting.

The proposal was revised to be more general and submitted for the September meeting and a committee vote. The new title is “Usage Guide for the INCITS RBAC Standard.”

THE HEALTHCARE SCENARIO ROADMAP Non-Licensed Personnel -Update

The task force assigned to prepare and submit the non-licensed healthcare portion of the permission catalog data is well underway having completed 98 of the 99 ASTM Non-Licensed Healthcare Roles. The RBAC Permission Definition Subcommittee continues to meet regularly to resolve issues based on departmental inputs from VA Medical Centers (VAMCs), DoD and IHS throughout the U.S. Input comes directly from licensed and non-licensed healthcare personnel in the field.

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

≈



STANDARDS CORNER

OASIS

Update coming soon

ASTM

Dates announced for upcoming meeting (see below)

ACM

Upcoming meetings (see below)

UPCOMING MEETINGS

- **ASTM E31 Meeting**
November 6-8, 2005
Dallas, TX
- **HL& Education Summit**
November 8-9, 2005
Boston, MA
- **ACM 12th Conference on
Computer Communications
Security 2005**
November 7-10, 2005
Alexandria, VA
- **ASTM Committees
D02, D03 and G02**
December 4-8, 2005
Norfolk, VA
(Meeting relocated due to
Hurricane Katrina)
- **HL7 Working Group
Meeting**
January 8-13, 2006
Scottsdale, AZ



eXtensible Access Control Markup Language (XACML)

In order to accomplish the goals of the RBAC TF effort, each enterprise must map the reference model to its own systems and for implementing standard permissions as specific instances of operations, on the enterprise information objects. If this mapping is done in a site or application-specific way, it may result in highly specific maintenance to encode and maintain each application. The eXtensible Access Control Markup Language (XACML) provides to developers the means to interface applications to a standard language for mapping standard permissions to operations on enterprise information objects. XACML is a markup language, based on an XML schema, used to express and evaluate access decisions on a system resource.

A more detailed explanation of the XACML information exchange is defined by the OASIS eXtensible Access Control Markup Language Version 1.0, which became an OASIS standard on February 6, 2003.

[Neumann Strembeck] provides a basis for defining roles using scenarios. Within this context, the following clarifications are made:

- Tasks reflect an organization's job functions and can be used to deduce permissions.
- The set of all work profiles a user is permitted to participate in reflects that user's functional roles.
- Basic roles determine a user's authorization to connect to protected resources.
- Permissions determine what operations a user is permitted on health information system protected resources.
- Permissions are assigned to functional roles.
- Standard functional roles consisting of grouped standard permissions are defined to support inter-domain data transfer.
- Standard permissions can be mapped to specific health information system operations and protected health information.
- Users will be assigned to functional roles according to the principal of least privileged.

The operational benefits of RBAC have long been recognized to assist in simplifying the complexity of managing user permissions in large networked environments, thus providing reduced administrative cost and time. RBAC is neither a new concept nor unique to the healthcare industry. Its implementation within healthcare systems however has been a challenge with a vast array of healthcare personnel roles and tasks, as well as the variety of non-homogeneous commercial and proprietary environments.



Health Information
ARCHITECTURE

Role-Based Access Control (RBAC) Newsletter



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

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

