



Inside this issue:

- **RBAC Review – Part II**
- **Notice: RBAC Task Force reconvening**
- **Health Level Seven (HL7) Security and Accountability Technical Committee – DSTU Ballot Update**
- **RBAC Website 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

≈

ROLE BASED ACCESS CONTROL (RBAC) – AN ABSTRACT REVIEW

Observations on the Real-World Implementation of Role-Based Access Control – continued from March 2006 Issue

Abstract written by Burkhard Hilchenback

RBAC Implementation

RBAC--per Mr. Hilchenback, is more a school of thought than a collection of software features. For companies, the implementation of RBAC means no less than the business process reengineering of their security administration. Starting from scratch is simple, but beginning in a complicated environment with dozens of security systems, tens of thousands of user definitions, and millions of authorizations, can be very difficult. Strictly speaking, the migration to RBAC is not within the scope of work of a standards organization such as NIST.

In RBAC implementation, thinking about the migration process in advance provides a lot of insight into the strengths or weaknesses of a standard and helps to make the standard widely accepted.

The necessity to deal with the migration process should be viewed as critical in that the initial situations of companies are very different and the process would be very difficult to standardize. Some identified common factors of successful migration to RBAC include:

- Each RBAC system must have the ability to load the existing security definitions ('Initial Load') and to administer them as they are. Systems that have to start from scratch or do not administer the old structures will not have the slightest chance of success. An incremental way for implementing RBAC on top of preexisting systems is needed.
- The link between role descriptions (in the company security policy) and the security systems leads to two approaches for RBAC implementation: starting from the policy side or from the security system side.

1. The top-down approach starts from the role descriptions. If there is no policy at all, we will start from scratch by defining all privileges that, for example, an EMT should have. A role EMT is created holding these privileges.



Upcoming Meetings

- **NIST and FISSEA Conference**
Training for a Cyber-Secure Future
March 20-21, 2006
Bethesda, MD
- **ASTM Committees E31 May 2006 Meeting (in conjunction w/TEPR)**
May 22 - May 24 2006
Baltimore, MD
- **HL7 Working Group Meeting**
May 7 — 12, 2006
San Antonio, TX
- **OASIS Symposium**
9-12 May
San Francisco, CA
- **11th ACM SACMAT 06 Conference**
June 7-9, 2006
Lake Tahoe, CA

≈

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

EMT IDs are connected to the role EMT and the role takes control over the existing privileges at the ID defined standard. The remaining privileges (that are not controlled by the role) are revised. The goal is to minimize the number of these privileges.

2. The bottom-up approach starts from an existing EMT definition. An EMT ID is searched whose privileges are as close as possible to a desirable standard, in creation of the VHA specific role (for example, the ASTM 1986E list was used). A role EMT is now created after this ID standard. The automatic creation of a role after an existing user ID is a feature each RBAC system should have. This EMT is now connected to their own role, which does not result in any modification of his/her privileges. Other EMTs are added, and again, the number of privileges that are not controlled by the role is minimized. Finally, the role is described as the de-facto standard for EMTs.

- A simple comparison of users that are supposed to have the same role (across say, hospital organizations) may show immense differences and may or may not be of help in the definition of the role.
- The best way to define roles, per Mr. Hilchenback, is to set up a taskforce consisting of 'old hands.' Their knowledge is the best source of information. A taskforce consisting of 'outsiders only' would not be efficient. It is also a bad idea to evaluate privileges by looking at their creation date and other kinds of 'historic' information. This data is always extremely misleading. Instead, the taskforce must set up an evaluation method that measures existing privileges based on the actual needs of a specific role. Traces of current privilege usage may be helpful.
- During the implementation of RBAC, user privileges are homogenized and simplified. In reality, this includes the deletion of superfluous privileges for users, often on a surprisingly large scale. A factor that should not be underestimated is the psychological effect this has on the users. Even if privileges are removed that are superfluous, questions arise as to why they were removed and employees may feel threatened.

The implementation of RBAC frequently opens up questions of a very general kind: What resources have to be secured and which



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

user attributes are security-relevant? The (often implicit) approach of companies to secure everything and to take everything into account leads to massive and unnecessarily complex sets of security definitions. RBAC asks for simplifications and the open discussion of these issues. At one of Mr. Hilchenback's customer sites, implementing RBAC led to a reduction of security-relevant user attributes from >100 to 5.

- The implementation of RBAC contains a lot of manual work. It is feasible to write generators that automatically create roles from existing user definitions. Yet, at this point, all generators are customized programs and program logic is heavily dependent on the specific (customer) situation. Large portions of the work will still remain manual.
- RBAC cannot be achieved by a stand-alone effort of the security administration department. Input from the organization department (role definitions, workflows, etc.), the human resources (HR) department (user data), and other departments is essential. The definition of roles will even sometimes affect the work of these departments. At one of our customers, the data HR was maintaining was slightly changed in order to serve as input for automatic, role-based creation of IDs. This had benefits not only for security administration, but also for HR.

Conclusions

The following issues should be carefully considered when designing a standard for RBAC:

- Roles are by their nature enterprise-wide. Standards for 'local' and 'global' RBAC may be desirable.
- The concepts of roles and groups intersect. There are good reasons to have both. Common grounds and differences should be documented well.
- The actual privileges of a user are composed of his/her role, individuality, and locality. A good RBAC system should support all three concepts.
- Roles must be able to cover all security-related definitions. This typically includes user and privilege attributes.
- Standards for handling intersecting and contradicting roles must be set. The progress of migration from one role to the other must be well defined.



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

- Privileges given to users directly will remain; roles can only minimize their number.
- Hierarchical relationships between roles are normally sufficient. Cardinality seems to be a rare requirement. The ability to handle exceptions is definitely necessary.
- The separation of duties is encouraged by RBAC and should be enforced by a RBAC standard.
- A description of the role engineering process is desirable in order to increase the acceptance of the standard. However, such a standard is difficult to write. We would prefer a standard that allows the creation of roles starting from existing definitions (bottom-up engineering).

References

- [1] John F. Barkley, "Implementing Role-Based Access Control using Object Technology," First ACM Workshop on Role-Based Access Control, Gaithersburg, MD 1995
- [2] John F. Barkley, Anthony V. Cincotta, David F. Ferraiolo, D. Richard Kuhn, "Role-Based Access Control in Large Networked Applications," National Institute of Standards and Technology, 1996
- [3] 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
- [4] David F. Ferraiolo, and D. Richard Kuhn, "Role-Based Access Control," 15th National Computer Security Conference, Vol II, pp 554-563 1992
- [5] SAM Customer Manuals, Release 2.1, Schumann Unternehmensberatung AG, 1995
- [6] Trusted Computer Security Evaluation Criteria, DoD 5200.28-STD, Department of Defense, 1985

RBAC Taskforce – Update

The RBAC Taskforce will be reconvening to discuss the addition of constraints to the current Permission Catalog and Roles. Members will be contacted with a meeting agenda when a meeting date has been set.



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

≈

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE

Draft Standard for Trial Use (DSTU) Ballot – UPDATE

The materials listed below were prepared and submitted to HL7 and voted affirmatively as a Draft Standard for Trial use in the January 2006 Ballot. Thank you again to all who contributed over the years to this major effort.

- 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, and
- HL7 RBAC Role Engineer Process Applied Example v1.1.

Updates and clarification have been addressed and made to remove the residual remaining negative comments to the overall DSTU. A resolution draft addressing the remaining negative comments to the above submitted documentation was distributed to those submitting the comments to review and a request made to remove their negative comment(s).

Role-Based Access Control is critically important to the security aspects of the VA and other healthcare organizations. There is a growing management and security demand for RBAC to be implemented in healthcare systems.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies.

The latest RBAC Documentation additions and prior RBAC Newsletters can be found on the RBAC Website; www.va.gov/RBAC. Please visit the newly updated site!!