



Inside this issue:

- ✦ RBAC Abstract Review – Part I
- ✦ Healthcare Scenario Roadmap – HL7 Update
- ✦ Health Level Seven (HL7) Security and Accountability Technical Committee – DSTU Ballot Briefing 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, Part I

Abstract written by Burkhard Hilchenback

Role-based access control (RBAC) is an emerging concept for security administration for large and decentralized computing environments. This abstract paper written by Mr. Hilchenback summarizes the experience of implementing RBAC at large corporations and compares it with the standards which were then suggested for RBAC. In addition, it briefly discusses issues relating to the migration from a conventional security administration to RBAC. The publication contains proprietary terms and registered trademarks of their respective owners. Careful observation and removal of such terms have been made. The review performed here is an examination of observations made by Mr. Hilchenback and their parallel to the current VHA RBAC business. Examples presented have been adapted to reflect VHA RBAC healthcare roles. This abstract text describes the relationship of a user to roles and groups with slightly different terms than those used in the VHA: a user is *connected* to a role, but the user is a *member* in a group. The examples cited have been adjusted to accommodate a healthcare system.

Security administration in large computer environments is a complex and expensive task. Many companies handle it by giving security administrators ownership of all data. If an update is required, a more or less automated workflow is in place to notify the administrator. This process is slow and error-prone.

RBAC is considered an alternative to mandatory and to discretionary access control. RBAC is actually a newer approach on how to organize privileges. It allows for data ownership, but the owner connects “their” data to roles rather than to actual IDs. Existing security systems already provide primitive elements of RBAC (e.g., user groups), but these features are fragmentary and are not standardized. The National Institute of Standards and Technology (NIST) is a driving force behind the move to standardize RBAC.



Upcoming Meetings

- ✉ **HL7 Educational Summit**
March 7 — 9, 2006
Chicago, IL
- ✉ **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

¹*RBAC as an Enterprise-Wide Task*

For corporations, roles are actually descriptions of job functions. In this example, roles may be defined to describe an “EMT,” a “Paramedic,” or a “Physician – Emergency Room.” In heterogeneous computing environments, a role description virtually always includes privileges across several platforms and within numerous applications. It is a difficult and time-consuming process to redundantly define roles and administer users across the enterprise. Per Mr. Hilchenback’s abstract, having a separate RBAC system on all the platforms is helpful, but would still require a lot of work: For example an EMT role would be needed on the Client/Server DBMS; another EMT role must be defined on the mainframe access control system, and so on.

The value of a comprehensive RBAC system may be fully realized when applied at the enterprise level. Here roles are by their nature are not limited to a single operating system or platform. Future standards may even define RBAC on two levels: A “local RBAC” standard for single applications and a “global RBAC” standard for enterprise-wide security administration systems.

Roles versus Groups

Many existing security systems support the concept of grouping. A group is a named collection of users. A group can hold a set of privileges to resources. Users may be members in one or more groups. A user that is a member in a group inherits the privileges of the group. Groups implement some aspects of roles as defined for RBAC. For example, a group called “EMT” can be used to implement the role of an Emergency Medical Technician. All Emergency Medical Technicians IDs belong to the “EMT” group. The question groups beg is this: Is RBAC essentially a very sophisticated kind of group concept, enhanced by features like group hierarchy, cardinality, dynamic and static separation, and others?

According to Mr. Hilchenback, groups are used for three different tasks:

¹ 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



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

1. Groups are used to collect sets of privileges that belong together in a technical sense rather than by the “semantics” of a role. A typical group contains all privileges required in order to run. This group is not a role, but it can be used by a role like “EMT.” Because an emergency medical technician needs to work under this group, the EMT role enforces the membership.

2. Groups are used to hold access rights that can be organized by an external hierarchy. An example of this is a geographical hierarchy.

3. The groups in a role hierarchy hold privileges and automatically inherit privileges from parent groups to child groups and finally to users. On the lowest possible level, access rights are given to single users for special tasks.

The RBAC standard as discussed in this abstract may accommodate the requirement that a role must be able to control every attribute or privilege which may be given a user in a security system. A role might look more like a template user than like a group in the traditional sense. This requirement could be called the “Rule of Completeness”: A role definition must be capable of completely holding all definitions that are needed to fulfill this role.

Role Intersections and Contradictions

In the RBAC approach of NIST, roles are exclusively utilized in order to grant privileges to users. As discussed previously, roles should also be able to handle user attributes. Even the privileges themselves have attributes: For example, privileges may allow specifying START-TIME and END-TIME. The privilege is valid only if used within the time range as specified by these values (for example, from 9 AM to 5 PM).

Mr. Hilchenback mentions that unfortunately, attributes add a new dimension of complexity to RBAC. Using an attribute like Shift-Time in the example, there are basically four ways a role can control its value:

- ✍ The role enforces an *explicit value*: All EMT have access starting from 9 AM.
- ✍ The role enforces that Shift-Time is *empty*: EMT access to this resource must not have a start time restriction.
- ✍ The role does *not specify anything* for Shift-Time: There may be a time restriction for a specific EMT given either from above, manually by the administrator or by another role, or there is no restriction.



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 role enforces a *value interval*: The Shift-Time for EMT may be between 7 AM and 10 AM, with a default of 9 AM. A role in an RBAC system should at least allow for definition of a specific value, or to leave the attribute unspecified. Attribute values lead directly to a second, larger problem: intersecting and contradicting definitions of roles. What if a user is member in the role EMT and the role PARAMEDIC, but both roles need to enforce a different START-TIME?

Role contradictions can also occur on a higher level. What if one role gives “write” access to a file, and another explicitly denies access to that file (explicit denials are a special case of privileges supported by most access control systems)? RBAC will have to handle intersecting and/or contradicting roles. The RBAC design of NIST contains the concepts of static separation (a user may not be connected to two roles at the same time) and dynamic separation (a user may not use the privileges of two roles at the same time). These concepts allow the administrator to describe certain mutual exclusions that will avoid many conflicts upfront. The design however, does not replace a well-defined conflict handling of the RBAC system for all the (very realistic) cases where the administrator is not aware of a conflict. The system behavior must be defined when a user changes the role, for example, from EMT to PARAMEDIC. What happens to all the definitions from the old role which are unspecified in the new role?

Definitions of the role are copied to the user and enforced at all times. This is great news for every auditor: only by looking at the role, he/she can tell which access rights all Emergency Medical Technicians (or Paramedics) have.

No system can actually force the administrator to work role-based; it can only support and simplify it. RBAC is primarily a school of thought, not a collection of tools. To our thinking, it will not be of much use to prohibit authorizations given directly to users.

Security maintenance does not have to take place at a central location and by one person. The RBAC concept encourages the decentralization of administration and the separation of duties. For example, the central security administrator defines and maintains the roles, while the decentralized administrators (e.g., the various emergency stations) use the roles to quickly administer IDs. This relieves the administrator from day-to-day work; first by the benefits of RBAC itself, but also by assigning the day-to-day work to decentralize administrators. The separation of duties is an important part of the total concept of RBAC.

To be continued in the next issue...



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

Complete References for the Abstract: *Observations on the Real-World Implementation of Role Based Access Control* are listed below:

John F. Barkley, "Implementing Role-Based Access Control using Object Technology", First ACM Workshop on Role-Based Access Control, Gaithersburg, MD 1995

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

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

David F. Ferraiolo, and D. Richard Kuhn, "Role-Based Access Control," 15th National Computer Security Conference, Vol II, pp 554-563 1992

SAM Customer Manuals, Release 2.1, Schumann Unternehmensberatung AG, 1995

Trusted Computer Security Evaluation Criteria, DoD 5200.28-STD, Department of Defense, 1985

RBAC TASK FORCE – Update

The RBAC Task Force will be reconvening in Spring 2006 to discuss the addition of both role and permission constraints to the current Permission Catalog and Functional Roles list. Members will be contacted with a meeting agenda when a meeting date has been set.

HEALTH LEVEL SEVEN (HL7) SECURITY AND ACCOUNTABILITY TECHNICAL COMMITTEE

Draft Standard for Trial Use (DSTU) Ballot – Update

The following list of materials were prepared and submitted to HL7 and voted affirmatively as a Draft Standard for Trial use in the January 2006 Ballot. Thank you 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.



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

NEWSLETTER NOTES

Article contributions and
submissions should be directed
to:
Suzanne.Gonzales-Webb@va.gov

Questions, comments or
corrections regarding this
newsletter? Please contact the
RBAC Newsletter editor.

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.
