Health Information ARCHITECTURE

Role-Based Access Control (RBAC) Newsletter

Volume 29 – July 2006

Inside this issue:

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

'*Modeling Privilege Management and Access Control*'

Kudos to our own Mike Davis for his contributions and co-authorship of this paper published in the International Journal of Medical Informatics.

Article Summary and Excerpts

The article introduces the basics of formal and generic modeling health-related security and privacy services to establish trustworthy health information systems. Its objective was to establish trustworthiness in advanced architectures for future proof health information systems to being open flexible, scaleable, portable and semantically interoperable. Security and privacy services needed must be designed as an inherent part of the architecture. Such architecture has to meet the paradigms of distribution, component orientation, formal modeling, separation of logical and technological aspects, etc.

Establishing an eHealth environment, organizational, legal, functional, social, ethical, and technical requirements must be met. In that context, security and safety are important challenges, influencing user acceptance and specifying risks which face healthcare establishments. In eHealth, only those professionals contributing to the patient's care shall be allowed to access extracts of personal medical records. Performing security analysis, risk assessment, policy specification, and Continuity of Business (COB) management, etc., narrative or semiformal methods are used. For analyzing health information systems and describing their security requirements, many standards, methods, and tools are available; however, these are not supporting the implementation and the enforcement of the security services needed. This obstacle needs to be overcome in order to achieve the realization of interoperability.

Over the last decade, the role-based access control (RBAC) paradigm has been developed and stepwise enhanced as the way of managing authorization and access control.[1] Permission assignment

[1] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youjan, Role-based access control models, IEEE Comput. 29 (2) (2001) 38-47 (February 1996)
http://doi.ieeecomputersociety.org/10.1109/2.485845

Upcoming Meetings

- **OASIS Co-sponsored XML Summer School**
  July 23-28, 2006
  University of Oxford, UK
- **OASIS Cosponsored Tri-XML Conference: XML in the Flow**
  July 27-30, 2006
  Raleigh, NC
- **HL7 Educational Summit**
  July 11-13, 2006
  Philadelphia, PA
- **HL7 20th Annual Plenary & Working Group**
  September 10-15, 2006
  Boca Raton, FL
- **ONC (ONCHIT)**
  American Health Information Community Meeting
  October 7, 2006
  Washington, DC 20201

ASTM Committees E31
November 12-14, 2006
Atlanta, GA

~

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

is based on the role a principal is assuming during a work session. Early work done by the authors has been validated and confirmed.[2]

The policy is bound to the role and not to the principal, thereby forming rather stable (static) relationships. For mutually exclusive sets of roles, simple rules, or constraints have been defined. Temporal RBAC and environmental RBAC have been used to manage more complex coarse-grained and rather simple security policies for meeting additional constraints. Richer security policies can be handled by the generalized RBAC defining ordered groups of subject roles, object roles, and environmental roles.

The weakness of all currently available RBAC models is the definition of simplified policies without ways for implementing and controlling them. If some enforcement has been realized, it has been borrowed by the inclusion of assumptions about the underlying technology; abstracting functionality. In any case, security services and functionalities are therefore not part of the application's behavior. The only way of combining security services and application functions is the integrated enforcement of security. As a solution, security services have to be designed as an integrative part of the application system's architecture.

Security needs definition. The definition of security needs and requirements can be properly done using a layered model of security concepts, services, mechanisms, functions, and algorithms. The algorithm layer provides the essential examples for cryptographic algorithms used for encoding, hashing, or signing information. For details refer to references.[3]

Roles may be assigned to any principal. Principals are the actors in healthcare. Therefore, roles are associated to actors and to acts (actions). For managing relationships between the entities mediated by an activity, two different roles have to be defined: organizational roles at the entity's side and functional roles at the act's (actions)

---

[2] G. Neumann, M. Strembeck, A Scenario driven role engineering process for functional RBAC roles, in: Pro-engineering process for functional RBAC roles, in: Proceedings of SACMAT'02, June 34, Monterey, CA USA, 2002 (ACM 1581134967/02/0006) http://doi.acm.org/10.1145/.507711.507717

[3] B.Blobel, F.Roger-France, A Systematic Approach for Analysis and Design of Secure Health Information Systems, Int. J. Med. Inform. 63 (3) (2001) 51-78, http://dx.doli.org/10.1016/S1386-5056(01)00147-2.

W. Stallins, Network and Internet Security. Principles and Practice, Prentice Hall, Hemel, Hempstead, 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

side. In general, two types of roles can be distinguished; rather static structural roles and highly dynamic functional roles.

Structural roles reflect the structural aspects of relationships between entities, whereas functional roles reflect functional aspects of relationships between entities. According to the HL7 approach and contrary to the UML specification, the association class is not bound to the association but has been represented by a class type in this figure, however. Considering both structural roles and functional roles in the same context, structural roles provide the prerequisites/competences for entities to perform interactions (an Act) within their specific functional roles. Qualifications, skills, etc. are influencing both the assignment of the structural roles and the performance of activities according to their functional roles. Possible examples for structural and functional roles of healthcare professionals are given in the table below:

Table: Examples for Structural and Functional Roles

Structural Role Examples	Functional Role Examples
Medical director	Caring doctor (responsible doctor)
Director of clinic	Member of diagnostic team
Head of the department	Member of therapeutic team
Senior physician	Consulting doctor
Resident physician	Admitting doctor
Physician	Family doctor
Medical assistant	Function-specific nurse
Trainee	
Head nurse	
Nurse	
Medical student	

Functional role model. Functional roles can be defined in levels of authorizations and access rights in the following generic way reusing slightly changed definitions established in the Australian HealthConnect Project[4], cross referenced against other works:

- Subject of care (normally the patient),
- Subject of care agent (parent, guardian, carer, or other legal representative),

[4] Australian Government, Department of Health and Aging, The Australian HealthConnect Project, http://health.gov.au.

~

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

- Responsible (personal) healthcare professional (the healthcare professional with the closest relationship to the patient, often his GP), and
- Privileged healthcare professional.

Another way for grouping functional roles according to the relation to the information created, recorded, entered, processed, stored, and communicated could be: Composer, Committer, Certifier, Authorizer, Subject of information, Information provider.

Another approach for structuring functional roles related to information and its use complying with the European Data Protection Directive and the related ISO CD 22857 ''Health Informatics Guidelines on data protection to facilitate trans-border flows of personal health information.''[5]

Structural role model. Structural (or organizational) roles (also called static roles) which place people in an organizational hierarchy as belonging to categories of healthcare personnel warranting differing levels of access control. Organizational roles allow users to participate in the organization's workflow (e.g. tasks) by job, title, or position but do not specify detailed permissions on specific information objects. Static roles allow a user to ''connect'' to a resource but do not grant authorizations. Some role group examples include: Physician, Pharmacist, Registered Nurse Supervisor, and Ward Clerk. Static roles may be found as non-critical certificate extensions entries to an X.509 certificate as specified in ASTM 2212-02 [34]. The term ''role groups'' is used for organizational or structural roles. Because the RM-ODP-based approach of different levels of granularity, grouping in the sense of generalization is applied to every component[6] (also functional roles can be grouped to role groups). Therefore, the term ''structural role'' or ''organizational role'' defined in the ISO standards framework seems to be more appropriate. Another critical aspect of terminologies used is the term permission to an Act. Harmonizing with the HL7 RIM, ''organizational roles'' for HL7s ''roles'' and

[5] ISO CD 22857 Health informatics, Guidelines on Data Protection to Facilitate trans-Border Flows of Personal Health Information.

[6] B. Blobel, R. Nordberg, Privilege Management and Access Control in Shared Care IS and EHS, in: R. Baud, M. Fieschi, P. Lebeaux, P. Ruch (Eds.), The New Navigators: From Professionals to Patients, Series Studies in Health Technology and Informatics, vol.95, IOS Press, Amsterdam, 2003, pp. 251-256

~

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

''functional roles'' for HL7s ''participation.''[7] See ASTM E1986-98 for a listing of healthcare personnel that warrant differing levels of access control.[8] A critical aspect of terminologies used is the term permission to an Act. Harmonizing with the HL7 RIM, ''organizational roles'' for HL7s ''roles'' and ''functional roles'' for HL7s ''participation'' to perform ''acts'' have been introduced. Resulting from a different approach to security services compared to the approach of architectural components used in this paper, permission with encapsulated operations and objects instead of the activity is used in NIST[9] and VA.[10]

New permissions will lead to a new role. The approach taken by the authors on policies bound to all basis classes to express conditions and rule on the one hand and permissions on the other hand is more promising and more consistent managing everything in the same generic way.

Most of the available solutions for defining and enforcing security and privacy solutions suffer from the weakness of the separation of definition and enforcement regarding underlying paradigm and the process, i.e. structure, functionality, methodology, accountability, specification, and processing languages, etc. The proposed paradigm has been developed over 10 years and demonstrated and evaluated in international projects. For the first time, security services have been directly embedded into the architectural components of health information systems using the same principles and the same process as for components' structure and functionality concerning any services. Already, since the beginning of the nineties, functional and structural roles have been defined and instantiated by the authors within several projects and initiatives. This status has been developed from the RBAC concept related to transactional steps of a workflow towards an architectural approach of security. For that purpose, a generic security model as well as a Generic Component Model for health information systems has been introduced in the

---

[7] B. Blobel, F. Roger-France, A Systematic Approach for Analysis and Design of Secure Health Information Systems, Int. J. Med. Inform. 62 (3) (2001) 51-78, http://dx.doi.org/10.1016/S1386-5056 (01)00147-2.

[8] ASTM E1986-98, Standard Guide for Information Access Privileges to Health Information.

[9] D.F. Ferraiolo, R. Sandhu, S. Gavrilla, D.R. Kuhn, R. Chandramouli, Proposed NIST Standard for Roles Based Access Control, ACTM Trans. Inform. Syst. Security 4 (August (3)) (2001 224-274

[10] VHA Security Architecture Framework, Enterprise Architecture 2001 Version, http://www.va.gov/OIT/EAM/EAservice

~

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

mid-nineties, which has subsequently been embedded into a completely model-driven approach for analyzing, specifying, implementing and maintaining health information systems.

The approach presented in this paper allows for the central management of users, privileges, rules, policies, separation of security management and secure application functions. It embeds security (policies as structural and functional constraints) into applications. Furthermore, it enables scalability of both security services and mechanisms on one hand and applications on the other. The approach separates AEF, ADI, ADC, etc.[11]

There are many solutions available for access control, and some work has been provided on privilege management. Some of the work has been dedicated to the healthcare domain. Currently, requirements and solutions for security services and especially application security services have been specified using narrative text, platform-specific or domain-specific expression means, however.

The paper integrates security services into a very advanced architectural framework using paradigms and methodologies in a model-driven architecture environment. Being involved in research and development including standardization for many years, the authors first introduced formal models to describe security requirements and solutions for advanced health information systems and especially the health systems' core application Electronic Health Record.

The presented results provide a framework for mapping the approaches published by different international and national teams as well as an approved basis for future-proof EHR systems and related applications model driven architecture environment.

Results. Currently, standards developing organizations are defining emerging tasks and standards for semantic interoperability and trustworthy collaboration for advanced health information systems. Communication security issues have been specified and implemented, while application security challenges such as a privilege management and access control are still under development. Therefore a series of formal models have been developed by the authors covering, e.g. domains, service delegation, claims control, policies, roles, authorizations and access control.

[11] Ibid, B. Blobel, R. Nordberg, Privilege Management and Access Control in Shared Care IS and EHS

~

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 required models are introduced and interpreted in a generic way. The crucial concept of security policy and its relationship to the other concepts have been considered in detail.

Conclusion. Based on formal models, security services can be integrated into advanced systems architectures enabling semantic interoperability in the context of trustworthiness of communication and cooperation.

Authors:

*Bernd Blobel - Fraunhofer Inst for Integrated circuits IIS, Health Telematics Project Group;

*Peter Pharow – Fraunhofer Inst for Integrated circuits IIS, Health Telematics Project Group, *Ragnar Nordberg – Sahlgrens University hospital, Gothenburg Sweden;

*John Mike Davis – US Department of Veteran Affairs, CISSP, SAIC, Veterans Health Administration, USA

http://vaww.cio.med.va.gov/OpenLinesWeb/readingRoom.htm

RBAC at SACMAT

ACM Symposium on Access Control Models and Technologies (SACMAT)

The SACMAT 2006 Symposium offered several novel research contributions in the current research of access control; specifically in technology, analysis, models and framework.

The Eleventh ACM Symposium on Access Control Models and Technologies (SACMAT). SACMAT 2006 is the eleventh of a successful series of symposia that continue the tradition, first established by the ACM Workshop on Role-Based Access Control, of being the premier forum for presentation of research results and experience reports on leading edge issues of access control, including models, systems, applications, and theory. The missions of the symposium are to share novel access control solutions that fulfill the needs of heterogeneous applications and environments and to identify new directions for future research and development. SACMAT gives researchers and practitioners a unique opportunity to share their perspectives with others interested in the various aspects of access control.

~

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

Papers offering novel research contributions in any aspect of access control are solicited for submission to the Eleventh ACM Symposium on Access Control Models and Technologies (SACMAT).

RBAC Taskforce – Update

The next RBAC Taskforce meeting call will be held August 2nd, 2006 - Wednesday at 1:00CT / 1100PST / 1200MT / 2:00EST.

The RBAC Taskforce will continue the discussion of additional of constraints to the current Permission Catalog and Roles. Members will be contacted with an agenda and additional materials in preparation for the meeting. If you would like to be a part of the Task Force please contact Suzanne Gonzales-Webb for more information, thank you.

~

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.