Role Standards in Healthcare

Edward J. Coyne
ed.coyne@med.va.gov

Amy B. Page
amy.page@med.va.gov

John M. Davis
mike.davis@med.va.gov

Dawn D. Rota
dawn.rota@med.va.gov

Science Applications International Corporation
and
Veterans Health Administration
U.S. Department of Veterans Affairs

ABSTRACT

Currently, there is widespread international interest in role-based access control (RBAC) as one form of policy-based access control. RBAC standards and numerous related papers from organizations such as the National Institute of Standards and Technologies (NIST), Association of Computing Machinery (ACM), Organization for the Advancement of Structured Information Standards (OASIS) and the International Organization for Standardization (ISO) are establishing fundamental principals for RBAC implementations. At the same time, efforts to develop essential domain-specific role content have not keep pace with the growth of standards.

The Department of Veterans Affairs (VA) Veterans Health Administration (VHA) has taken the lead in promoting role engineering processes supporting standard role definitions for healthcare organizations. VHA role-engineering efforts began more than two years ago with the formation of two distinct RBAC Task Forces, one including several healthcare partners and one internal to VHA. The scenario-based role engineering process resulting from this work was subsequently vetted through both Task Forces. Based largely upon earlier work by Gustaf Neumann and Mark Strembeck [1], VHA adopted engineering and role definition content models complying with those of the American National Standards Institute (ANSI) RBAC standard [2].

This paper describes the goals, approach, results, and lessons learned from our healthcare role engineering work.

Keywords

Role Engineering, Access Control, Basic Roles, Functional Roles, RBAC, Healthcare, Permissions, Security.

1. INTRODUCTION

The Department of Veterans Affairs is engaged in a large multi-year project to implement comprehensive identity and access management as part of a larger service-oriented security infrastructure. The Veterans Health Administration decided to adopt role-based access control as the means to define healthcare security policies used by this infrastructure. Two needs in this regard were recognized: (1) an enterprise-wide set of roles that would be semantically compatible across a portfolio of applications and (2) interoperability of access control among VHA and its business partners, which also implies a degree of standardization within the healthcare community. To achieve these needs, a consistent process for defining roles, permissions, constraints, and hierarchies would be needed.

The goal throughout the effort has been to standardize role names and permissions through recognized standards bodies such as such as the National Institute of Standards and Technologies (NIST), Association of Computing Machinery (ACM), Organization for the Advancement of Structured Information Standards (OASIS) and the International Organization for Standardization (ISO). This is in recognition, gained through VHA, DoD and other's experience, that enterprise proprietary role definitions would not suffice for business-business interoperability and secure health information exchange.

We distinguished early-on between the functional roles described by the ANSI RBAC standard [2] and basic roles as defined by Bernd Blobel in [3]. We extended the definition of basic roles to mean those that are a prerequisite to initiating a session or, within a session, to connect to a resource such as an application.

A national Healthcare RBAC Task Force (TF) comprised of healthcare personnel and healthcare informatics

specialists from several organizations was established. The Healthcare RBAC TF had representation from VHA, Indian Health Service (IHS), Department of Defense (DoD), and Kaiser Permanente (KP). The Healthcare RBAC TF validated the role engineering process and is promoting the adoption of this process and the standardization of basic role names and functional healthcare permissions within several standards development organizations.

ASTM Standard E1986-98, *Standard Guide for Information Access Privileges to Health Information* [4] was selected to characterize basic role names. As the process was applied, additional healthcare personnel actors were identified or clarified. These modifications were submitted to ASTM for possible inclusion into the standard.

Since scenarios are key to the role-engineering process a source of healthcare-specific scenarios was needed. Two scenario sources were ultimately decided upon: 1) adoption of previous work accomplished by HL7 (Health Level Seven) Technical Committees (storyboards); and 2) documentation resulting from facilitated sessions of the VHA RBAC TF. The healthcare scenarios and discussions were then used within the process to develop a catalog of abstract high-level healthcare permissions forming the basis for final scenario generation and creating permissions with greater granularity.

Within VHA, the work of deriving permissions is being extended to identifying functional role names with associated permissions. It is expected that other organizations would conduct a similar effort to relate the permissions in the permission catalog to enterprise-specific role names once HL7 standard permission definitions are published.

The figure below illustrates Functional Role, Permission, and Operation and Object relationships adapted from the ANSI RBAC Core RBAC reference model. It does not include the concept of basic roles or sessions, which are not part of the RBAC TF role engineering process.

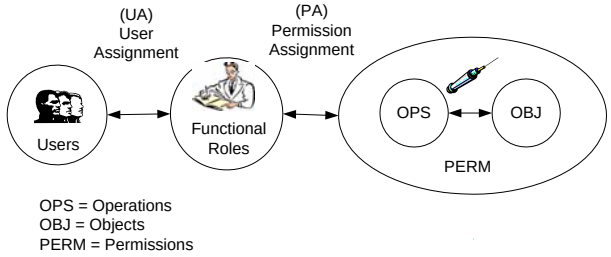

Figure 1. Role Structure (Adapted from ANSI RBAC Core RBAC Model)

In an effort parallel to that of the VHA RBAC TF, the existing VHA VistA healthcare information system is being reverse engineered to derive implicitly defined functional roles. The roles so identified will be compared to the permission aggregations of the role engineering effort to achieve a harmonization of the two. This effort is expected to result in a VHA-specific functional role set.

2. RELATED WORK

In developing their scenario-driven role-engineering process, Neumann and Strembeck [1] conducted three case studies that have assisted them in refining the process. Anecdotal evidence from several sources points to attempts to define roles for an organization that have been less than successful. Reasons given for these outcomes include underestimating the level of effort required and difficulty in achieving consensus on role definitions. The present project has purposely chosen to reduce scope to a minimum to avoid the anticipated obstacles to success.

3. THE SCENARIO-DRIVEN ROLE ENGINEERING PROCESS

3.1. Description of the Process

Neumann and Strembeck summarize their general approach in the scenario-driven role engineering process as follows:

1. Identify and model usage scenarios
2. Derive permissions from scenarios
3. Identify permission constraints
4. Refine scenario model
5. Define tasks and work profiles
6. Derive preliminary role hierarchy
7. Define RBAC model

The Scenario Model, as shown in the figure below, illustrates the hierarchy of work profile, task, scenario, and step. Permissions are defined relative to steps (described in the role engineering process to follow).

In the scenario-based role-engineering approach each action and event within a scenario can be seen as a step that is associated with a particular access operation. Scenarios, which are applied in a particular order to reach a predefined task goal, act as sources for the derivation of permissions. The user performing a scenario must own all permissions that are needed to complete every step of the scenario.

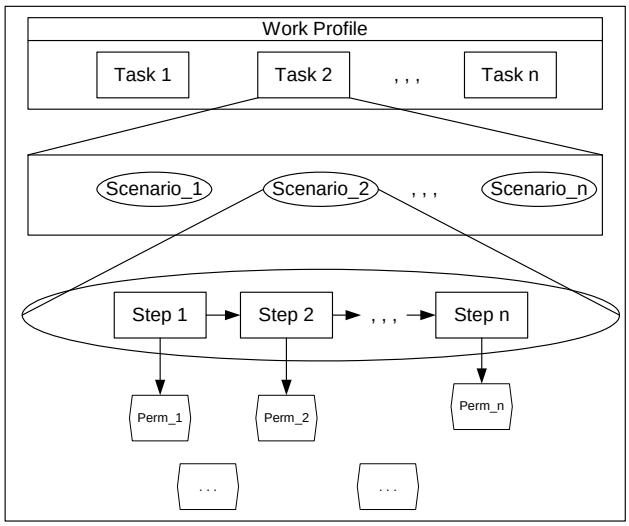

Figure 2. Scenario Model [Neumann/Strembeck]

For the initial effort, steps six and seven were deferred to the anticipated stage when individual organizations would create enterprise-specific roles. The early belief that the role engineering process would represent a significant effort, and that therefore the goals should be relatively modest, was borne out in practice. This foresight was based on the knowledge and input from the healthcare domain experts involved in the effort.

3.2. Modifications Made by VHA

The role engineering process was formally reviewed by the Healthcare RBAC TF and approved for use with some modifications and clarifications. Assumption, constraints and process tailoring occurred.

The following initial assumptions were made regarding the activities of the VHA RBAC TF.

- Scenarios are documented as Unified Modeling Language (UML) sequence diagrams.
- Defining the RBAC model means the identification of standard permissions.
- Explicitly naming functional roles based upon standard permissions is not desired.
- Initial activities of the RBAC TF will not include role-role constraints.
- All permissions will be defined in relation to HL7 Reference Information Model (RIM) Version 3.0.

The actual process used by the VHA RBAC TF to identify permissions is as follows:

1. Create or adopt/adapt a natural language scenario that describes a healthcare workflow.
2. From the scenario description, prepare a UML sequence diagram that captures actors and actions. See figure below.
3. In the UML diagram, identify where interactions with an information system occur. These are called steps.
4. Identify permissions required to perform each step. Enter the permissions into a permission catalog.
5. In the permission catalog, combine permissions that are considered to be duplicates.

Optional:

6. For each permission, refine it to actual system access control terms, e.g., CREATE, READ, UPDATE, DELETE, EXECUTE.

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

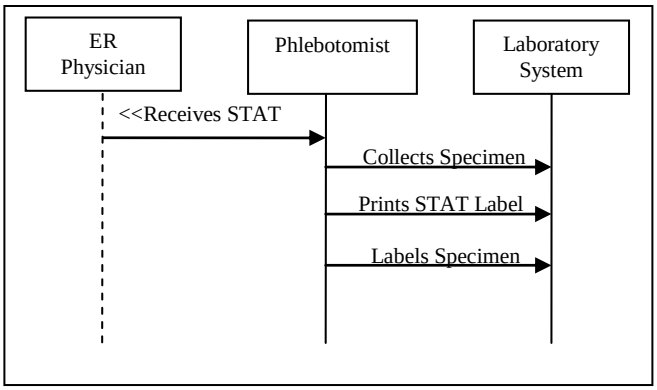

Figure 3. UML Sequence Diagram Example

- 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 operational roles.
- Basic Role groups 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 may be used to define functional roles.
- Standard functional roles composed of 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 are assigned to functional roles according to the principle of least privilege (inherent in the workflow-scenario approach).

3.3. Approach to Implementing the Role Engineering Process

Task Force Makeup. The VHA TF was comprised of healthcare personnel, security and technical role engineers. The members were a dedicated team that included physicians, nurses, pharmacists, security architects, developers and analysts. The TF Chair was a physician with considerable organizational and interpersonal skills along with a familiarity in information technology (IT). Several other members were also very conversant in Federal Health Insurance Portability and Accountability Act (HIPAA) guidelines, Federal security requirements, IT and related policies. In addition, some TF members have experience in other specializations such as healthcare informatics and participate in standards development organization activities.

The role engineers were from the VHA Health Information Architecture (HIA) Office. Their expertise was in the areas of IT and security. They had hands-on experience with selecting and tailoring the role engineering process. The Functional Analyst Lead of the role engineering effort was both an IT software engineering professional and a Registered Nurse. The role engineers assisted the healthcare domain experts by creating artifacts to contain and display the results of the effort. The Functional Analyst Lead also provided a vital communication function by maintaining a role engineering website and producing a monthly newsletter.

Communication Mechanisms. Weekly teleconferences were the primary medium used by the Healthcare TF for conducting its activities. The agendas for the teleconferences were distributed in advance and minutes were prepared and distributed soon after the teleconference.

The VHA RBAC TF held face-to-face meetings approximately every six months. The meetings primarily focused on RBAC strategy, the Healthcare Scenario Roadmap, basic roles and the RBAC architecture.

An RBAC website dedicated to the TF's activities was established to contain the VHA RBAC TF artifacts as well as other relevant references such as technology papers and newsletters.

RBAC e-mail groups were used to disseminate information to all parties who expressed an interest in RBAC. There are a few different RBAC e-mail groups such as: the Healthcare RBAC TF, the VHA RBAC TF, the VHA business partners and outside interested parties. Emails are sent on a regular basis regarding the latest RBAC happenings.

A newsletter was developed and distributed to all interested RBAC parties on a monthly basis. The newsletter contained pertinent Standards Development Organization (SDO) information and synopses of the latest RBAC research papers and standards information. The newsletter always contained a hyperlink to the RBAC website.

Exit Criteria. Exit criteria were defined and used as guideposts to indicate when the task force goals were met in a satisfactory manner. Since this was a collaborative effort, the collaboration was needed to collectively evaluate the adequacy of satisfying the defined exit criteria. All TF deliverables were evaluated with the following exit criteria:

Completeness	• Did the goal or work product cover all recognized topics? • Were these topics covered adequately?
Correctness	• Were all parts of the goal or work product free from significant errors?
Internal Consistency	• Were all parts of the goal or work product consistent with each other?
External Consistency	• Were all parts of the goal or work product consistent with other accepted sources?
Generality	• Was the goal or work product free of ad hoc assumptions and locally defined components?
Simplicity	• Were the parts of the goal or work product free of complex language or analysis that may impede the document's use?

3.4. Work Method of the Task Force

Scenario Identification. Two sources of healthcare scenarios were used: HL7 storyboards and facilitated sessions with the VHA RBAC TF members. The storyboards, provided courtesy of HL7, consisted of fictitious settings representing typical healthcare encounters and related IT functions. The storyboards were not ideal as healthcare scenarios for three reasons: 1) they represented the activities of multiple actors which is contrary to the role engineering process; 2) they did not provide adequate coverage of healthcare activities; and 3) historically, HL7 has been a messaging standard so use of these storyboards was not an easy fit. However, as used to identify permissions and not roles, they were adequate to "prime the pump" for the effort. As a result, the task force was able to "fill-in-the-gaps" and create scenarios to complete the coverage of the healthcare domain.

Step Identification. Each scenario was modeled as a UML sequence diagram. In the scenario-based role-engineering approach each action and event within a scenario can be seen as a step that is associated with a particular access operation. Scenarios, which are applied in a particular order to reach a predefined task goal, act as sources for the derivation of permissions. The actor performing a scenario must own all permissions that are needed to complete every step of the scenario.

Permission Identification. Scenario steps in the diagrams were ultimately represented as both an abstract permission and a basic permission. Permission identification includes reviewing each scenario step and deciding which operation a user needs to perform to complete this step. The basic permissions as described in the ANSI RBAC standard are denoted by {operation, object} pairing. These pairs were considered to be common in healthcare applications. Subsequent activities included a normalization process whereby duplicate permissions were consolidated and renamed. In this process of engineering the permissions, an audit trail of the engineering activities was maintained in case it might be necessary to revisit some of the consolidation decisions.

Abstract Permission Name	Basic Permission Name
Receives STAT Order	{R, Order}, {C, Observation}
Collects Specimen	{U, Observation}, {U, Order}, {R, WorkList}
Prints STAT Label	{C, Device}
Labels Specimen	{C, Container}
Arrives Specimen	{U, Observation}, {U, Order}
Processes Specimen	{U, Observation}
Logs Specimen	{U, Observation}
Notifies Order	{U, Observation}, {U, Order}

4. RESULTS OBTAINED

4.1. Basic Roles

The VHA RBAC TF reviewed and adopted the list of "Healthcare Personnel That Warrant Differing Levels of Access Control" contained within ASTM Standard E1986-98 as basic roles. The standard list of 16 licensed healthcare personnel from the ASTM standard was used to map the healthcare personnel to four high-level and 74 detailed clinical activities performed by licensed healthcare providers. Furthermore, a comprehensive cross-index of the ASTM standard was made to relevant personnel defined by the National Uniform Claims Committee.

During the mapping process, the VHA RBAC TF noted that in some cases healthcare personnel within the existing standard were not as comprehensive nor as consistent as they needed to be for the role engineering work.

In May 2004, the VHA RBAC TF presented recommended revisions to the *ASTM E-1986 Standard Guide for Information Access Privileges to Health Information* list of "Healthcare Personnel that Warrant Differing Levels of Access Control" to the ASTM E31 Committee. The VHA RBAC TF provided 14 licensed healthcare personnel categories and a hierarchical sub-category within some of those over-encompassing licensed healthcare personnel with 34 licensed sub-categories. The ASTM E31 Committee accepted the proposed modifications for future balloting.

4.2. Healthcare Scenario Roadmap

Early on in the process, the VHA RBAC TF recognized that the effort of identifying work tasks and profiles for all healthcare personnel (licensed, non-licensed and non-caregiver) was daunting. In order to scope the effort, a spreadsheet called the Healthcare Scenario Roadmap, was created as a foundational tool to assist in defining the scope of the RBAC modeling effort, as well as be utilized as a quick reference of healthcare scenarios. The roadmap presents scaleable management of user permissions in the form of a list of tasks as a healthcare standard.

The figure below illustrates a portion of the Healthcare Scenario Roadmap. The 'x' axis shows the preliminary roles. The abstract permissions are shown on the 'y' axis. The intersecting cells containing an 'x' indicate preliminary roles that are generally authorized to perform

the corresponding abstract permission, while cells containing an 'o' indicate preliminary roles that generally are not authorized to perform the corresponding abstract permission. For instance, the intersection of abstract permission 'New/Change/Discontinue Laboratory Order' and preliminary role 'Dentist' indicates with an 'x' that this role performs this abstract permission. Each of the cells containing an 'x' is recorded within a scenario or work pattern and sequence diagram(s).

Legend: **x = performs** **o = does not perform** **? = unknown**	**Audiologist**	**Dental Hygienist/Registered Dental Hygienist (RDH)**	**Dentist (DDS or DMD)**	**Dietitian (RD)**	**Non-western Medicine Providers**	Certified Acupuncturist (CA)	Licensed Massage Therapist (LMT)/Registered Massage	**Nurse**	Clinical Nurse Specialist (CNS)	Clinical Registered Nurse Anesthetist (CRNA)	Licensed Vocational Nurse (LVN)/Licensed Practical Nurs	Nurse Midwife (NM)	Nurse Practitioner (NP)	Registered Nurse (RN)
Order Entry														
New/Change/Discontinue Laboratory Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Radiology Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Renew/Change/Discontinue/Refill Outpatient Rx Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Inpatient Medication Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Diet Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Consult Order	x	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Nursing Order	o	o	x	o	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Standing Order(s) PRN	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Verbal and Telephone Order	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Supply Order (e.g. ostomy, diabetic)	o	o	x	x	o	o	o		x	x	x	x	x	x
New/Change/Discontinue Prosthetic Order (e.g. wheelchair, crutches)	o	o	x	x	o	o	o		x	x	x	x	x	x
Sign Order(s)	o	o	x	x	o	o	o		x	x	o	x	x	x

4.3. Permission Catalog

Application of the role engineering process to the healthcare scenarios results in a catalog of abstract permissions. This artifact is a list of tasks, permissions, operations, and objects for healthcare roles. For each of the operations, a record containing an {operation, object} pair is defined, e.g., {write, progress_note}. Examples of using the process to develop a permission catalog were developed and provided to HL7 as a framework for a draft healthcare RBAC standard.

4.4. Permission-Permission Constraints

Where appropriate, constraints between permissions were recorded as part of the process. For example, a constrained permission occurs when only one role is allowed to perform a particular task at any given time. A constraint occurs for a permission when its' definition is tied to cardinality. In this case, the constraint on the permission would be the cardinality specification. Examples of permission constraints include:

- Head Nurse on a hospital floor (cardinality of one)
- Chief of Staff (cardinality of one)
- Lab Technician vs. Lab Technician Supervisor (separation of duties)
- Provider's access to a remote hospital which is not his/her primary workplace(location)

- Physician working in a clinic (time-dependency) vs. physician working in the ER (no time-dependency)

4.5. Functional Roles

The national Healthcare Task Force did not undertake the definition of role names. This was to be the province of enterprise-level task forces. However, it proved useful to use a candidate set of role names as placeholders for the actor in a scenario prior to generalization. The TF decided to use the ASTM basic role names as a candidate set to facilitate the work of the TF. This dual-use of the basic role names as a placeholder for the actor resulted in some confusion among the participants in the process. In reality, the basic roles were simply being used temporarily as surrogates to prime the discussion and analysis.

4.6. Significance of Results

Among the results obtained by the role engineering effort was the achievement of a practical, verifiable and repeatable role engineering process. This single step greatly enhances the feasibility of extending the standardization effort to SDOs such as HL7 and ASTM. Through this work, the goal of achieving inter-organization interoperability among international healthcare organization at the permission level is beginning to be realized.

In May 2004, the Healthcare RBAC TF presented a proposal to the HL7 Board of Directors at the HL7 Working Group Meeting held in San Antonio, Texas. The HL7 Board of Directors approved the adoption of the RBAC effort (i.e., the specification of permission definitions as a healthcare standard) into its family of standards. In taking on this effort, HL7 is leveraging its large and active healthcare domain expertise to create a single international healthcare standard for interoperable RBAC. Recent RBAC activities were also presented to other HL7 Special Interest Groups (SIGs) and Technical Committees (TCs), including the Security and Accountability SIG, Government Projects SIG, Personnel Management TC, and Clinical Context Object Workgroup (CCOW) TC.

5. LESSONS LEARNED

5.1. General

Organization. A national task force was convened to identify and promote the standardization of healthcare permissions. These standard permissions were intended to be used as building blocks by disparate organizations in creating healthcare roles. It was decided not to attempt to standardize on role names at the national level, as the roles with their assigned permissions would be unique to each organization. A VHA organizational role engineering task force was convened for purposes of creating roles that are local to VHA. It should be noted that there was considerable overlap of personnel between the national and VHA task forces.

Charters for the two task forces were prepared for approval by management. This approval was obtained within VHA and had a positive effect on the continued availability of resources.

RBAC Task Force Charter

TABLE OF CONTENTS

Scope
- 1.1. Business Case
- 1.2. Objectives
- 1.3. Customer Needs
- 1.4. Work Products
- 1.5. Customer Requirements
- 1.6. Exit Criteria
- 1.7. Scope Boundaries

Assurance
- 1.8. Scope Risk Limit
- 1.9. Reviews and Approvals
- 1.10. Communications

Resource Limits
- 1.11. Team Composition
- 1.12. Deadline
- 1.13. Task Force Constraints

Resources. A project management plan was developed for the VHA RBAC TF in an attempt to assign schedule and resources to the effort. This plan was not that effective in that most of the resources were on a part-time voluntary basis, not a dedicated resource. As expected, the role engineering effort was slow given this type resource allocation.

Role engineering is a labor-intensive undertaking. Sustained availability of subject matter experts and technical staff is a prerequisite to any successful project, especially one in which the principal product is semantic content. Failure to secure adequate resources is a major risk factor.

Scope. Because of the need for adequate resources and the enormity of the domain, it is necessary to limit the scope by defining initial objectives of the role engineering task forces. As stated earlier, this effort was scoped to "licensed healthcare providers in a clinical setting" as the minimal essential objective. In addition, scoping the initial objectives to match the expertise of the members of the task forces proved to be advantageous. In our case, the

expertise lay in the area of physicians, nurses and pharmacists.

One finding early in the efforts of the RBAC task force was that a distinction should be made between security functions and business rules. For example, task force members tended to want to include business rules in the permissions being defined given their knowledge of the VHA existing VistA healthcare system. A decision was reached that only security-relevant permissions would be identified, at least initially, to limit the amount of work that would be required to produce useful results. As mentioned earlier, other limitations imposed on the effort were to postpone the identification of role-role constraints and role hierarchies. However, permission-permission constraints were included in the process to capture these initially and avoid the need to make a second pass through the permission catalog to identify these constraints.

5.2. Makeup of Task Force

As stated earlier, the TF included healthcare workers and was led by a practicing physician. We believe this was most essential in achieving a satisfactory result of our initial objectives. While we believe this TF makeup to be necessary, in practice it may not be totally sufficient, in that such a group is not infallible. Subsequent review of the results is required by a broader base of healthcare knowledgeable individuals. To this end, technical committees within HL7 are now scheduled to verify and validate the initial results.

It is also recognized that in the future, when other parts of the healthcare domain are addressed, expertise from those areas (e.g. clergy, admissions, housekeeping) will need to be represented.

5.3. Need for Scoping

The goal of the national TF was to identify healthcare permissions that could be standardized. Thus, standard role names were omitted from the national goals. The motivation for standardizing permissions was to achieve a degree of inter-enterprise interoperability.

Since the identification of role names with associated permissions was to be accomplished by the enterprise task force, the following items were deferred in the national effort:

- role-role constraints
- role name assignment (except for basic roles)
- role hierarchy definition

5.4. Maintenance of Momentum of Task Force

The momentum of the TF was nurtured primarily through the weekly teleconference calls. These calls gave the TF an opportunity to work as a team in defining the permissions, discuss work tasks, make assignments and resolve issues. The minutes of these meetings are still referred to on a regular basis.

In addition, the monthly newsletter proves to be an effective communication mechanism for any interested RBAC parties. Emails are regularly received from persons all over the world.

5.5. Obstacles Overcome

The following obstacles were overcome in the execution of the RBAC effort:

- Sub-optimal assignment of staff to TF
- Translation of technical and clinical jargon and concepts between healthcare providers, security engineers and architects

Even though the assignment of staff to the TF was minimal and insufficient to address the entire healthcare domain, the re-scoping of the project to “licensed healthcare providers in a clinical setting” proved successful. The TF members were able to focus on their areas of expertise so that they were not overwhelmed by unfamiliar healthcare tasks.

In the area of communications between the architects and the healthcare providers, the architects had to learn to provide technical information in a way that was understandable to all members of the TF. The situation went both ways. Clinicians were sometimes required to explain clinical scenarios and terminology such that architects could understand the concepts. This was most apparent during discussions regarding security functions and business rules.

6. FURTHER DEVELOPMENT

While the primary goal of the healthcare role engineering task force has been to develop a permission catalog for healthcare roles, areas for additional development were discovered during the role engineering process. A realization was made that, beyond identifying roles and their permissions, was a need to identify related business rules and constraints. The VHA is developing an architecture within which healthcare permissions, constraints, and business rules will coexist within a common environment. In this architecture, enterprise policy, with security policy as a subset, will be represented as a system of rules. The results of evaluating these rules

will be available to all applications for use in making access control decisions.

7. DISCUSSION

The work of the Healthcare RBAC TF is in the process of being taken over by HL7 and its technical committees. With the acceptance of RBAC permission definitions into the HL7 family of standards, there will be many process and organizational changes that occur within HL7. The members of the Healthcare RBAC TF will continue to stay involved in the HL7 effort through both clinical and security related channels. For example, one RBAC TF member is currently co-chair of the Security and Accountability Special Interest Group.

While waiting for the HL7 effort to begin, the VHA RBAC TF is continuing its work in the non-licensed and non-caregiver areas. Input from various departments and software development groups within VHA are currently being solicited. In addition, the enterprise VHA RBAC TF is being re-organized and dedicated resources will be assigned to the effort. Finally, the reverse engineering of roles from the legacy VHA healthcare information system continues to mitigate the risk of creating any gaps in the new content definition.

8. CONCLUSION

The goal of developing and demonstrating a role engineering process and to institutionalize it within a standards-based permission definition effort has been achieved. The role engineering process can be applied equally to other domains. Defined healthcare permissions are obviously useful only within the context of interoperating health information systems. Our results were achieved through a significant effort at inter-organizational collaboration and cooperation, a sound and repeatable process, and by carefully focusing the efforts of limited resources on specific and clearly defined objectives. Having well qualified resources available, even if only part-time, was also a key success factor.

In the future, the Healthcare RBAC TF and the VHA RBAC TF will continue their work by focusing their collaboration within standards development organizations, applying the role engineering process to define additional permissions, identifying a complete set of basic roles, defining enterprise-level functional roles and refining a service-oriented healthcare-oriented privilege management infrastructure supporting RBAC as well as other types of policy-based access control rules. The goal is to ultimately have both an interoperable architecture and a common healthcare permission catalog capable of provisioning and implementing RBAC among all healthcare providers.

REFERENCES

[1] G. Neumann and M. Strembeck. *A Scenario-driven Role Engineering Process for Functional RBAC Roles*, June 2002.

[2] Information Technology Industry Council. *American National Standard for Information Technology - Role-Based Access Control*, ANSI INCITS 359-2004, 2004.

[3] B. Blobel. *Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems* (2002). IOS Press, 2002.

[4] American Society for Testing and Materials. *ASTM Standard E1986-98: Standard Guide for Information Access Privileges to Health Information*, 1998.