A Composite RBAC Approach for Large, Complex Organizations

Joon S. Park*
School of
Information Studies
Syracuse University
Syracuse, NY, USA
jspark@syr.edu

Keith P. Costello
School of
Information Studies
Syracuse University
Syracuse, NY, USA
kpcostel@syr.edu

Teresa M. Neven
Maxwell School
of Public Affairs
Syracuse University
Syracuse, NY, USA
tmneven@syr.edu

Josh A. Diosomito
Maxwell School
of Public Affairs
Syracuse University
Syracuse, NY, USA
jadiosom@syr.edu

ABSTRACT

Secure and effective access control is critical to sensitive organizations, especially when multiple organizations are working together using diverse systems. To alleviate the confusion and challenges of redundancy in such a large, complex organization, in this paper we introduce a composite role-based access control (RBAC) approach, by separating the organizational and system role structures and by providing the mapping between them. This allows for the explicit identification and separation of organizational and target-system roles, role hierarchies, role assignments, constraints, and role activations, with an attempt to bridge the gap between the organizational and system role structures. The composite RBAC approach supports scalable and reusable RBAC mechanisms for large, complex organizations. Our research explores the newly created Department of Homeland Security (DHS) as a large, complex organization in which the Composite RBAC can be applied.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection – *Access Controls*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Unauthorized Access*

General Terms

Management, Security

Keywords

RBAC, role-based access control, role mappings, role structures

1. INTRODUCTION

The tragic events of the September 11th terrorist attacks serve as a constant reminder of the imminent vulnerabilities this nation faces. Failures in strategic planning, information sharing, and state of readiness were all contributing factors that forced the federal government to re-evaluate its national security policies.

In an effort to prevent further terrorist attacks and better protect our nation's borders, President George W. Bush created the Office of Homeland Security in October of 2001. With overwhelming support from Congress, this executive office officially became the new Department of Homeland Security (DHS) in November 2002. This remarkable legislation represents the largest government reorganization since 1947, when the separate military divisions were consolidated into one agency, the Department of Defense. Similarly, over 22 government agencies are now consolidated into one agency, the Department of Homeland Security. The National Strategy proposed in July 2002 states the primary objectives as:

- Prevent terrorist attacks in the United States;
- Reduce America's vulnerability to terrorism; and lastly
- Minimize the damage and recover from attacks that do occur.

These goals have been and continue to be monitored by the collaborative efforts of multiple government agencies working together and sharing data sources. Two critical components to address in these consolidation efforts include:

- Strategic planning of research and development regarding security needs; and
- Cooperation of inter-government agencies to collect and disseminate pertinent intelligence information.

While these goals complement each other, in this paper we devise and creatively think of potential solutions that can ensure a greater degree of information sharing that is both more effective and efficient than at present, while still addressing the security concerns intrinsic to the organization. In the midst of coordinating agencies' roles and missions, much consideration will be focused on delegation of tasks and assignments with scalable access control mechanisms. Prior to the formation of DHS, one of the primary reasons and potential roadblocks to information sharing was the redundancy of existing data and intelligence resulting from multiple independent stovepipe operations. To mitigate these challenges, multiple agencies that once shared similar missions

* This work was supported in part by the "Information Assurance for the Intelligence Community (IAIC)" program of the Advanced Research and Development Activity (ARDA) and the New York State Center for Advanced Technology in Computer Applications and Software Engineering (CASE).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SACMAT'04, June 2-4, 2004, Yorktown Heights, New York, USA.
Copyright 2004 ACM 1-58113-872-5/04/0006...$5.00.

under different departments (e.g., Departments of Treasury, Justice, and Transportation) are now consolidated into one clearinghouse agency, the Department of Homeland Security.

To alleviate the confusion and challenges of redundancy in such a large, complex organization, we introduce a composite role-based access control (RBAC) approach, separating the organizational and system role structures and providing the mapping between them. RBAC has been selected because it is policy-neutral and allows for scalable collaboration while ensuring least privilege, separation of duties, and other constraints. We propose that there should be a separation of organizational and system level role structures to support scalable and reusable RBAC approaches for large, complex organizations such as DHS

This paper is exploratory research into how role-based access control (RBAC) might be implemented to provide system roles within a large, complex organization with pre-assigned organizational roles. Our approach also provides a secure and efficient access control to information for the multiple organizations (e.g., different government organizations) of which one hybrid organization is comprised. Our research provides a framework for a new composite role-based access control approach and discusses how a large, complex organization could implement RBAC effectively. As an example in the following discussion, we will consider DHS as an organization and a generic document authoring, publication, and management system (DAPMS) as a system.

While creatively thinking of measures to increase efficiency and efficacy of access control at DHS, we acknowledge several challenges. First, there presently exists a societal anxiety about potential opportunities for the abuse of authority (i.e., insider threats [21]) caused by such a system. As such, attention needs to be paid to the prescription of adequate safeguards and access restrictions to achieve and balance political and organizational objectives. This is complicated by conflicting interests among stakeholder groups in both the immediate and macro environments. Second, cost has a positive correlation to the level of assurance. While DHS wants strong security, there are both performance and capital costs that constrain their options. Third, the unique nature of consolidating 22 government agencies into one organization has never been attempted; there are no official standards, protocols, or guidelines to integrate these systems.

Despite these challenges, our research will help advance the study of RBAC within a large, complex organization such as DHS. Our research can assist policy makers and researchers on how to theoretically approach this issue, as well as advocate the importance of this topical area in future academic study.

2. RBAC (ROLE-BASED ACCESS CONTROL) OVERVIEW

The basic concept of RBAC is to "establish permissions based on the functional roles in the enterprise, and then appropriately assign users to a role or a set of roles" [2, 7, 9]. As illustrated by Figure 1, these roles are assigned to users, and permissions are associated with roles—not users directly. RBAC is policy neutral, and, as such, is not limited to specific types of organizations.

The benefit of RBAC to system administrators is the ability to assign permissions to dynamic populations of users based on their roles. Consequently, RBAC provides a mechanism for reducing the cost, complexity, and the potential for access control errors.

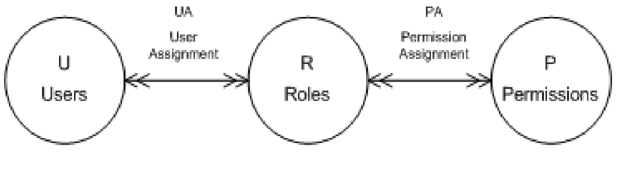

Figure 1: Flat RBAC

From the initial conceptions of RBAC, a family of RBAC models (RBAC'96 Model) was developed in 1996 by Ravi Sandhu and associates [2]. This model was in turn adapted to be the NIST unified standard RBAC model in 2000 [7]. The NIST model outlines cumulative levels within the 1996 model, characterizing them as flat, hierarchical, constrained, and symmetric. Park identified the user-pull and server-pull RBAC architectures and implemented them with secure cookies and digital certificates [9, 22, 23].

3. SEPARATION OF ROLE STRUCTURES

The Department of Homeland Security (DHS) possesses very different access control policy requirements as compared to commercial enterprise or the military. To accomplish the organization's missions, more effective and scalable access controls should be implemented that provide required constraints and flexibility. We believe RBAC is one of the most suitable solutions for achieving the access control requirement within DHS. One of the most useful benefits of RBAC is its ability to assign roles to dynamic populations of users. This reduces the one-to-one mapping that typically accompanies assigning users to permissions directly. Within a department comprising over 170,000 employees, administering the typical identity-based access controls can be a tremendous task.

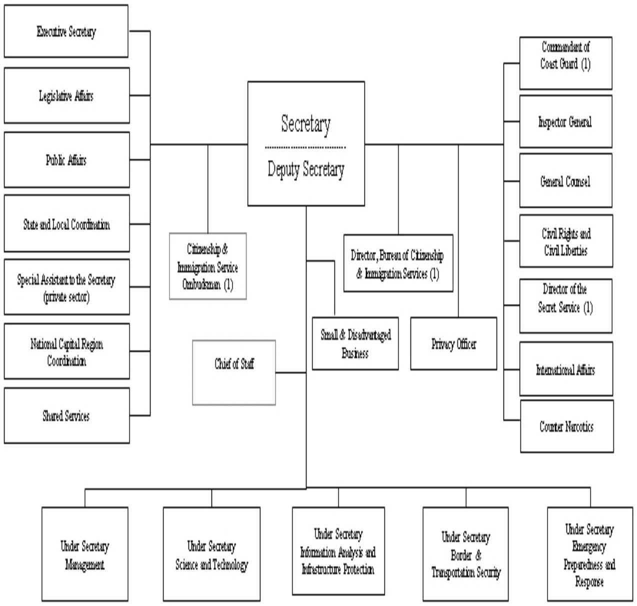
Executive Secretary
Legislative Affairs
Public Affairs
State and Local Coordination
Special Assistant to the Secretary (private sector)
National Capital Region Coordination
Shared Services
Secretary
Deputy Secretary
Citizenship & Immigration Service Ombudsman (1)
Chief of Staff
Director, Bureau of Citizenship & Immigration Services (1)
Small & Disadvantaged Business
Privacy Officer
Commandant of Coast Guard (1)
Inspector General
General Counsel
Civil Rights and Civil Liberties
Director of the Secret Service (1)
International Affairs
Counter Narcotics
Under Secretary Management
Under Secretary Science and Technology
Under Secretary Information Analysis and Infrastructure Protection
Under Secretary Border & Transportation Security
Under Secretary Emergency Preparedness and Response

Figure 2: DHS Organizational View

Secure and effective information sharing is mission critical to the organization. The intent of consolidating 22 government agencies into one organization (depicted in Figure 2) is to streamline the intelligence information gathered against potential terrorist attacks. Without a high-level security policy that stipulates guidelines and protocols, information sharing cannot be fully achieved.

Benefits of processing shared information across multiple agency levels in a timely manner can prove critical to the success or failure of DHS. If intelligence is gathered regarding potential terrorist activities, appropriate DHS representatives can assess the threat, devise a security plan to alleviate the risk, and delegate tasks accordingly. The delegation of tasks and inter-agency communications to share intelligence is mission critical. The overall goals of DHS are to prevent, detect, and respond to terrorist threats. Similarly, a sound security policy to ensure the safe transmission of shared information must be able to identity vulnerabilities, devise protective countermeasures, and respond accordingly [6].

Information sharing goes beyond exchanges of documents between individuals and line managers. Information sharing extends to organizations, both on national and regional levels. For instance, organizational communication between the Federal Bureau of Investigation (FBI) and Transportation Security Administration (TSA) can be to share information regarding vulnerabilities to potential terrorist activities to hijack an airplane. Information can then be disseminated region-wide where a threat specifically targets one area, in which information must be shared with designated security officials.

We believe the Composite RBAC approach, which supports scalable and reusable RBAC mechanisms (by separating the organizational and system role structures and providing the mapping between them), can support the needed access control requirements for such case. Access control goes beyond the organizational level and applies to diverse and numerous target-systems within DHS. Individuals should be provided with the minimum level of permissions necessary to perform their organizational and system roles. Applying the Composite RBAC approach within DHS and its systems would protect critical information and grant permissions to those whose roles require access to vital information.

3.1 An Example Scenario: DHS Information Flow

This section demonstrates one example of how information flows within DHS. Intelligence gathered from multiple government agencies is used to produce a series of documents. Documents include: security briefings, threat analysis, urgent memoranda, the President's Daily Briefing (PDB), and so on. Documents are then filtered accordingly to respective directorates within the department through the application of a document authoring, publication, and management system (DAPMS).

A plausible scenario of how intelligence is produced, filtered, and disseminated to respective directorate divisions of DHS is depicted in Figure 3. This visualization is limited to information being collected from the intelligence community and distributed to various agencies within DHS. The bi-directional arrows displayed on the chart demonstrate the capabilities of information being shared both ways. Shared information can flow between the sub-directorates and directorates, directorates and senior management, and most importantly between DHS and intelligence agencies.

As Figure 3 illustrates the information flow originates from either an intelligence or DHS. The intelligence reports are created, modified, forwarded, or transmitted by a DAPMS. The intelligence reports are issued in various forms. Some organizations issue security briefings, others issue memoranda or alert warnings, while some reports are collected and presented in the President's Daily Briefing (PDB). Once the report is collected and analyzed, pertinent information is filtered and disseminated by the DAPMS.

The information received from either the intelligence community or DHS is then readily available in a web-based document system. Based on the assigned roles and corresponding permissions, authorized users will be able to view intelligence reports. Depending upon the nature of a report or sensitivity, the report will then be administered by DHS. From there, an organizational hierarchy is formed. Hypothetically, the Secretary and Under Secretary will have access to all documents and reports. Based on the risk assessment of the intelligence reports, information would be assigned to one of the five directorates: *Information Analysis and Infrastructure Protection (IAIP), Border Transportation and Security (BTS), Emergency Preparedness and Response (EPR), Science and Technology (DST)*, and *Management*. These five directorates represent the very backbone of the agency's mission-critical objectives.

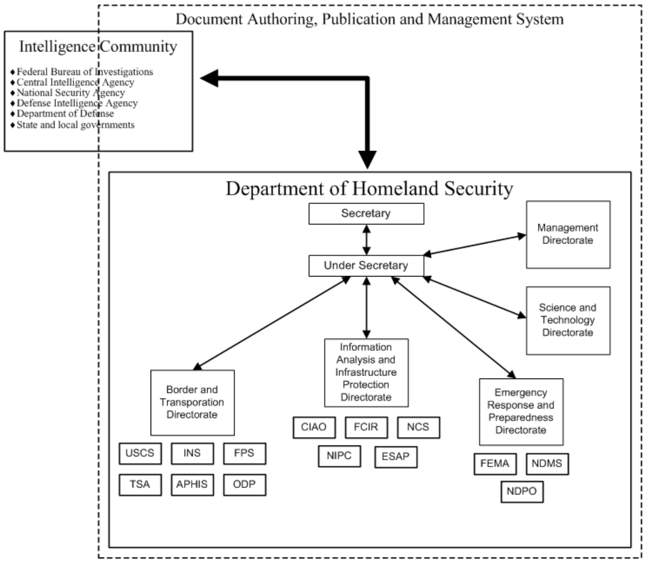
Document Authoring, Publication and Management System
Intelligence Community
♦ Federal Bureau of Investigations
♦ Central Intelligence Agency
♦ National Security Agency
♦ Defense Intelligence Agency
♦ Department of Defense
♦ State and local governments
Department of Homeland Security
Secretary
Under Secretary
Management Directorate
Science and Technology Directorate
Information Analysis and Infrastructure Protection Directorate
Border and Transporation Directorate
Emergency Response and Preparedness Directorate
USCS
INS
FPS
TSA
APHIS
ODP
CIAO
FCIR
NCS
NIPC
ESAP
FEMA
NDMS
NDPO

Figure 3: Information Flow within DHS

In summary, effective and scalable access control is pivotal to the success or failure of DHS. Establishing proper information flow and incorporating proper access controls ensure that the information generated is disclosed only to authorized users. The Composite RBAC approach would provide DHS with the necessary tools to accomplish the primary missions of the organization: to prevent terrorist attacks, reduce vulnerabilities, and minimize the potential administrative errors.

3.2 Access Control Parameters at DHS

Numerous access control parameters should be taken into account when implementing RBAC to a DAPMS at a large, complex organization. These include the organization's constraints as well as classes of roles. These classes of roles can be characterized as *organizational roles*, *system roles*, and *enterprise roles*.

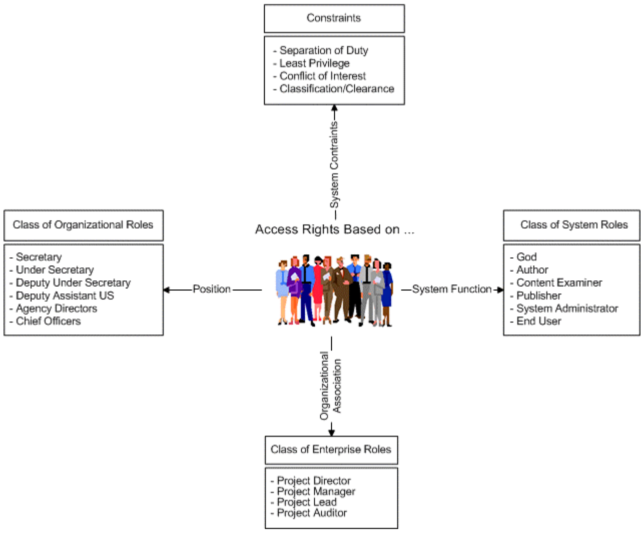

Figure 4: Access Control Parameters at DHS

The *class of organizational roles* reflects an individual's location in the organizational hierarchy. The *class of system roles*[1] is assigned based on the user's job function within a target system. In our example, the class of system roles includes the roles in the DAPMS application. The *class of enterprise roles* is for an enterprise project that spans multiple organizations and applications for a collaborative project [10, 11] such as project director, project manager, etc. Finally, *constraints* provide prescribed security rules for allowing and disallowing access. The major elements of each of the above roles, as well as the identified constraints as they relate to a DAPMS in this environment, are provided in Figure 4.

The focus of this particular paper mainly concerns the constraints, the organizational roles, and the system roles. Other researchers may develop different role hierarchies or other components of access control parameters for DHS than the ones presented in this paper; however, our objective is to establish a theoretical framework that demonstrates a separation of organizational and system role structures and the mapping between them. For the purposes of simplicity, we consider only one large, complex organization and one system in this paper. Any actual implementation would be more complex, as it would need to take into account enterprise roles that span multiple organizations, as well as the possibility of implementing across multiple systems.

3.2.1 Class of Organizational Roles at DHS

The class of hierarchical roles at DHS reflects the organization's natural role hierarchy, as depicted in Figure 5. Represented in this diagram are a few executive-level roles for each of the three directorates outlined in the prior section. The intent of this diagram is not to demonstrate the full complexity of the DHS organizational structure, but to provide an example of the hierarchical structure needed for implementing the organizational role hierarchy component of the Composite RBAC approach.

From the top of the diagram, the head of the organization is the *Secretary*. All authority and authorization would be included in this role. Below the Secretary is the *DHS Under Secretary* who is responsible for assisting the Secretary. In this example, there are three *Directorate Under Secretaries* who are in charge of the corresponding agencies of their directorates. The Under Secretaries for Border & Transportation Security (B&TS), Information Analysis and Infrastructure Protection (IAIP), and Emergency Preparedness and Response (EP&R) are represented here.

At this level, the Directorate Under Secretaries have *Assistant Secretaries* who report to them. Together, these leading executives direct and manage the agency *Directors*, *Administrators*, *Commissioners*, and *Assistant Attorneys General*. Additionally the leaders of these agencies are responsible for those within their domain.

As Figure 5 exemplifies, the hierarchy structure for implementing RBAC within DHS would need to follow a similar pattern in structuring organizational roles (This is an advantage of using RBAC). Lower tiered roles have less privilege than higher tiered individuals.

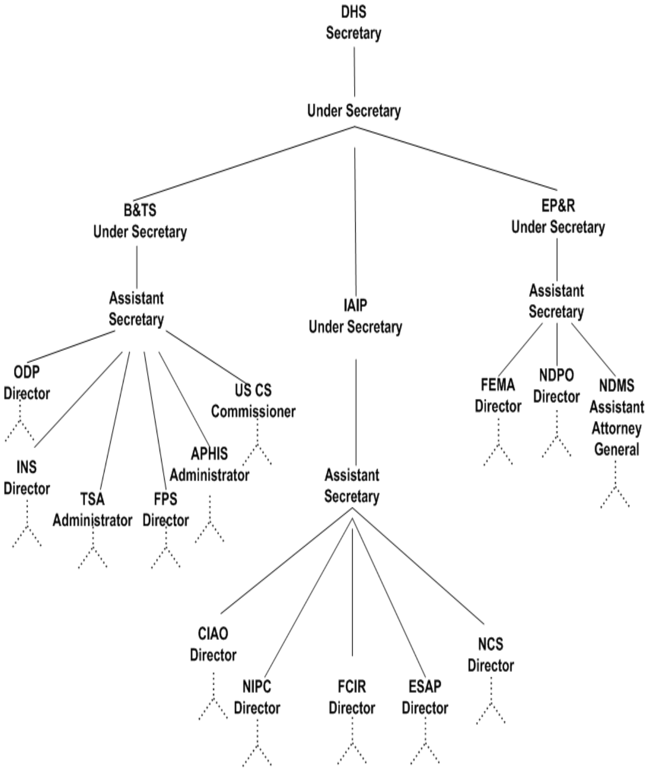

Figure 5: DHS Organizational Role Hierarchy

3.2.2 Class of System Roles in DAPMS

The class of system roles for the document authoring, publication, and management system (DAPMS) is *end users*, *authors*, *content examiners*, *publishers*, *system administrators*, and the system *god*. These roles form a role hierarchy within this system, as depicted in Figure 6.

[1] We can classify the system roles into the application roles and OS roles [21]. According to this classification, the roles in a DAPMS belong to application roles.

The system *god* is the single most powerful role within the DAPMS. Created at setup, the god role is the master account for the system, possessing a complete set of its permissions. While it may be omnipotent, the design of the god role is to facilitate role-role administration[2] within the system. If DHS chose to centralize access control to all its various systems, the god level role could be used as the interface to facilitate role-role administration tasks such as assignment and revocation. Next down the hierarchy is the *system administrator*, who is responsible for maintaining the DAPMS. The system administrator has the same abilities as the system god minus the privilege to perform role-role administration. This includes capabilities such as making modifications to the information architecture and content presentation of the front- and back-end interfaces, and auditing the logs of the DAPMS. The *publisher's* role is to interface with the back-end to assign documents to subject headings and to make documents available within the front-end interface once a *content examiner*, whose role is to review the validity and accuracy of the reports, has reviewed and cleared them. *Authors* play a key role in the DAPMS by creating and developing content for reports. They may reside within DHS; may be external government agencies, such as the NSA, CIA, or FBI; or may be other public or sector entities (e.g., CERT). The *end user* is at the bottom of the system role hierarchy, reflecting his/her status as the consumer of the DAPMS, interacting solely with the front-end.

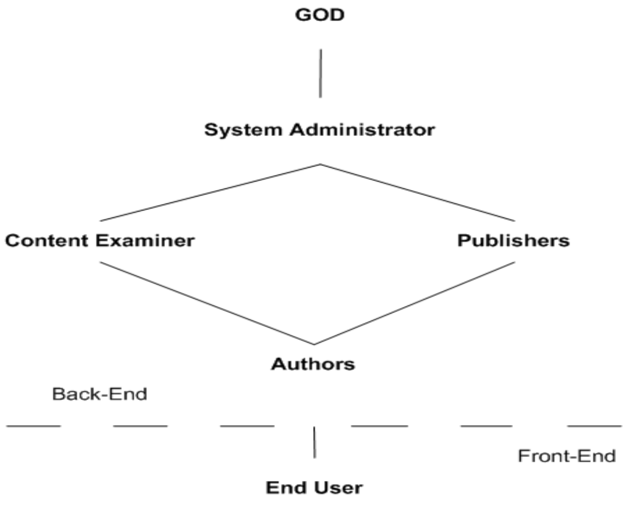

Figure 6: DAPMS Role Hierarchy

3.2.3 Class of Enterprise Roles

Enterprise roles are the roles that can be assigned for a collaborative project (usually, on a temporary basis). For instance, in Figure 4, these roles include: *Project Director*, *Project Manager*, *Project Lead*, and *Project Auditor*. A *Project Director* is responsible for overall planning, implementation, and evaluation of the project. A *Project Manager* is responsible for implementation, delegation of assigned tasks, and the daily operations of the team. A *Project Lead* is responsible for managing the project team, collecting data, and reporting to the Project Manager. Lastly, the *Project Auditor* is responsible for performance evaluation.

Enterprise roles can be assigned by an organization to the members of a task force. For instance, the enterprise roles could be assigned to a FEMA (Federal Emergency Management Agency) task force deployed to a disaster site to assess the physical damage of a hurricane. Likewise, the same roles could be assigned to a TSA (Transportation Security Administration) task force to assess the effectiveness of new metal screening detectors. For the purpose of simplicity and clarity, the current work on the Composite RBAC approach has placed less emphasis on enterprise roles, focusing more on the well-defined organization and system level roles. While enterprise roles are important to the implementation of RBAC and we describe their meaning, we assume that such roles can follow a similar framework outlined in this paper and our previous work [10, 11].

3.2.4 Constraints

Constraints are applied to both the organization and systems levels. These constraints may include *least privilege*, *separation of duties*, *conflict of interest*, and *classification*. The first three are common security policy principles, while the last has been highlighted due to the nature of the implementing organization (i.e., DHS) and of the specific target system in question (i.e., the DAPMS). Virtually any condition can be a constraint. Thus, there are other constraints that can be applied, depending on the specific circumstances of the implementation.

Least privilege is provided by RBAC and allows DHS to maintain the confidentiality and integrity of its data by ensuring that users have only the capabilities they absolutely need to have in order to perform a given task. In the DAPMS, least privilege is applied at each layer within the role hierarchy and reflects the specific permission needs of each role.

Separation of duties (SOD) ensures that mutually exclusive responsibilities are not authorized to the same person. For example, due to the application of the separation of duties constraint in our dynamic Composite RBAC approach, a user who has activated an author role cannot simultaneously activate the role of content examiner, as those two roles are mutually exclusive via the dynamic separation duties. Although for our intended target system all SOD constraints are dynamic, we acknowledge that other target systems will afford both static and dynamic role assignments.

Conflict of interest refers to the ability to influence or access information that would help promote one's self interests. Due to the extensive involvement and collaboration with external organizations in both the public and private sector, it is important for DHS to enforce access control constraints to guard against potential impropriety stemming from the disclosure of sensitive information to competing organizations that might result in a conflict of interest.

Finally, *Classification* is another form of constraint to protect against unauthorized disclosure and modification of sensitive information. Currently, the federal government grants people one of four security clearances authorizing them to access objects possessing classification less than or equal to their clearance. These classifications and clearances, in ascending order of sensitivity, are: unclassified, confidential, secret, and top secret. In the DAPMS, user clearance and document classification are

[2] For simplicity, in this example, the system role hierarchy contains both administrative roles and regular roles. Alternatively, we can maintain separate role hierarchies for those roles as described in the ARBAC model [3].

mandatory requirements to maintain the proper levels of integrity and confidentiality of its information.

4. MAPPING BETWEEN ORGANIZATIONAL AND SYSTEM ROLE STRUCTURES

To assist DHS in implementing RBAC for its various systems, the Composite RBAC approach provides the separation of role structures (described in Section 3) and the mapping between them (depicted in Figure 7). Our approach builds off of the existing RBAC components of user-role assignments (URA), role hierarchies (RH), permission-role assignments (PRA), selective role-activation (sessions), and constraints.

Most RBAC approaches typically consider the role structures within a single domain or multi-domains at the same level (e.g. between organizations or between systems). This is certainly of great benefit, but does not provide the necessary explicitness required to integrate RBAC into a comprehensive solution filled with numerous distinct systems and organizations. In real computing environments, basically we have two separate domains that we need to consider for effective access controls: organizations and systems. In order to make the RBAC approach more applicable, the need for considering role structures among multi-domains at different levels (e.g., between an organization and a system) as well as at the same level is pressing. This makes the current role-based approaches much more scalable, effective, and reusable.

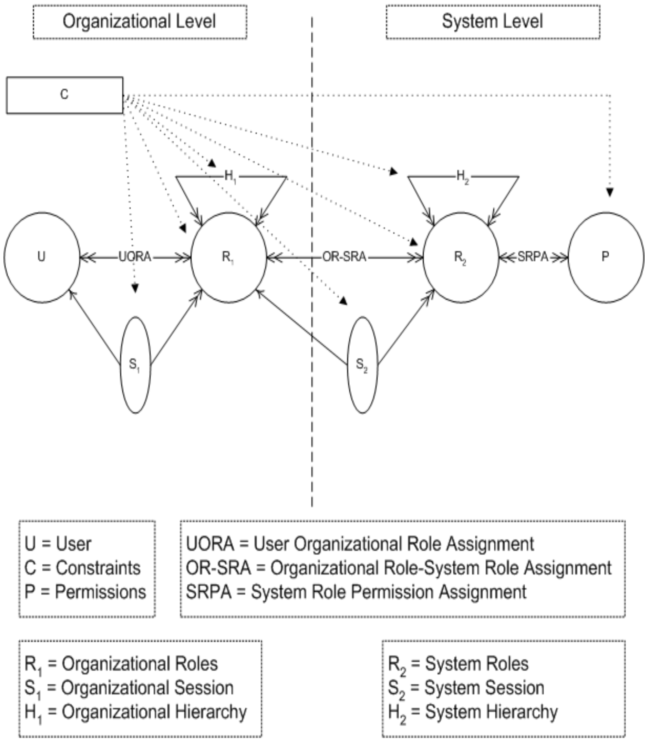
Organizational Level
System Level
C
H1
H2
U
UORA
R1
OR-SRA
R2
SRPA
P
S1
S2
U = User
C = Constraints
P = Permissions
UORA = User Organizational Role Assignment
OR-SRA = Organizational Role-System Role Assignment
SRPA = System Role Permission Assignment
R1 = Organizational Roles
S1 = Organizational Session
H1 = Organizational Hierarchy
R2 = System Roles
S2 = System Session
H2 = System Hierarchy

Figure 7: Mapping between Organizational and System Role Structures

The Composite RBAC approach is composed of two discrete hemispheres: organization and target-system. This distinction affords the capability of independent organizational and target-system role hierarchies, role assignments, and role activations (sessions) at these two levels. Users (U) are assigned to a set of organizational roles (R_1) commensurate with their job functions as well as their positions within the organizational hierarchy (H_1). This is the process of user organizational role assignment (UORA). Similarly, the target system may also have its own system hierarchy (H_2) of system roles (R_2). Via system role permission assignment (SRPA), these system roles are each associated with a set of permissions (P) within the target system. These two assignment processes (UORA and SRPA) are bridged by the organizational role-system role assignment (OR-SRA), which associates organizational roles (R_1) with target system roles (R_2). This is key, since different individuals will possess different roles within different target systems.

When a user activates a legal set of organizational roles based on the user's current task, signified by session S_1, this activated set of organizational roles (R_1) constrains the available set of system roles (R_2) within a given target system. The corresponding system roles in R_2 are activated via another session (S_2). This second activation, the activation of target system roles, provides mappings between the organizational and system roles. It also provides a means to enforce constraints (C)—such as separation of duty, conflict of interest, and least privilege—at a finer granularity. Typically, to use some applications in an organization, a user should be assigned to some organizational roles. For instance, a user, Alice, can be assigned to the system role Users because she has an Employee role in the organization, not because of her identity.

The role structure from each domain (organization or system) can be used as an interface when one role structure is integrated with others. This increases the reusability of the access control mechanism. The assignments among users, organizational roles, system roles, and their sessions effectively form a scalable and reusable net to control access in large, complex organizations.

Constraints (C) are applied equally across the partition, but are depicted as being driven by the organizational security requirements to reflect their origination from the organization's high-level policies. Such constraints work towards preventive security mechanisms that dictate the access parameters of both the organizational and target-system role. An example of how constraints can be applied to the Composite RBAC approach is illustrated in the section to follow.

4.1 Systems Level Permissions

The ultimate objective of access control is to acquire permissions for a given target system, rather than to merely associate them with an organizational role. This is significant, as organizational roles do not specify what rights and privileges a role should have at the target system level, therefore, are insufficient to describe the valid permission set at that level. Consequently, organizational role permissions have not been included in Figure 7. Instead, users who have activated a given organizational role then instantiate another session (S_2) that enables them to activate a target system role and acquire that system role's set of permissions.

4.2 OR-SR Assignment

The new concept of OR-SRA is applicable across various large organizations and is important for administering system roles that are both dynamic and flexible. OR-SRA mapping enables a finer granularity of access control through the increased ability to apply constraints with greater specificity.

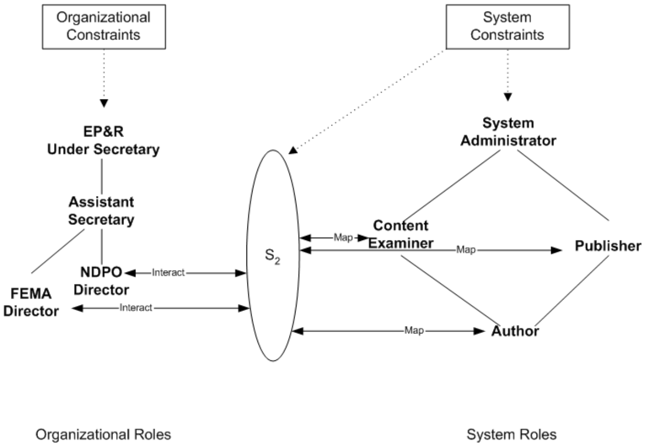

Figure 8: OR-SR Mapping Example

The mapping of roles between the organization and target system—the process of organizational role-system role assignment (OR-SRA)—is depicted in Figure 8 within the context of a DAPMS at DHS. The line managers, FEMA and NDPO Directors, represent the roles from the Emergency Preparedness and Response (EP&R) Directorate. Both organizational roles (FEMA and NDPO Directors) can be assigned to the same user. Both have the ability to activate a session (S_2) in which specific systems roles are assigned based on the purpose of their access. Figure 8 illustrates the organizational role of the FEMA Director interacting with S_2, which facilitates the mapping to system roles such as author, publisher, or content examiner. Similarly, the NDPO Director organizational role is also mapped via S_2 to a set of system roles. If both FEMA and NDPO Directors are activated in the same organizational session (S_1) by the user, all those corresponding activated system roles are in the same system session (S_2). Otherwise, each organizational role is mapped to its own system session. As illustrated in Figure 7, attached to each of the system roles are a series of permissions and corresponding constraints.

By mapping the organizational and system roles, role hierarchies, assignments, and activations are identified. This separate but integrated view allows for greater flexibility between each of the roles when a target system is changed and allows the mapping of pre-existing organizational roles to be applied to new systems. Conversely, the same target-system role structure can also be applied to any of the other directorates within DHS. Therefore, the mapping illustrated in Figure 8 will allow the FEMA Director to assume roles within the system needed to access secured documents pertaining to FEMA can be disseminated across subdivisions of the directorate or other directorates based on the policies. Likewise, the NDPO Director will be capable of authoring, examining, publishing, and being system administrator for the NDPO-related items within a DAPMS. Additionally, the Assistant Secretary of ER&P may assume the roles of both FEMA and NDPO Directors. The following section applies the concepts of constraints to the scenarios illustrated in Figure 8.

4.3 Impacts of Constraints

The mapping of organizational and system roles via OR-SRA is a key process for maintaining access control, and is dependent on the application of constraints. Established by high-level security policies to prevent or limit access control, these conditions can be characterized as organizational or system constraints. As illustrated in Figure 8, organizational constraints are applied to the organizational role hemisphere, while system constraints are applied to the system role hemisphere. The following examples are provided to illustrate the impact of constraints on the mapping of organizational and target-system roles in a DAPMS at DHS. It is important to note that only dynamic constraints are enforced during OR-SRA Static constraints are enforced during the creation of pre-defined organization-system role mappings.

Suppose the Assistant Secretary of Emergency Preparedness and Response (EP&R) needs to interact with the DAPMS to examine and publish content related to FEMA, as well as publish NDPO material awaiting his/her approval. Based on the application of least privilege at the user behavior level, the Assistant Secretary should activate only the roles that convey the permissions that are necessary to perform the task—thus, the Assistant Secretary should activate a subservient organizational role such as one at the Director level to perform his/her work with the DAPMS. Although the Assistant Secretary is capable of assuming all the roles below his/her position on the role hierarchy, such as FEMA and NDPO Director, s/he is restricted from using these organizational roles simultaneously due to the separation of duties between these two agencies. This is an organizational constraint that has been outlined in the organization's high-level policies. Therefore, the Assistant Secretary will need to activate these roles one at a time to perform these activities in the DAPMS.

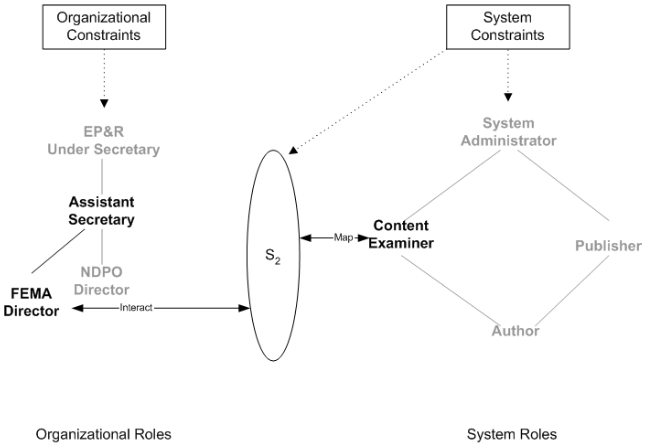

Figure 9: FEMA Director – Content Examiner Mapping

Once the organizational role is activated, additional constraints are then applied at the target-system level. By activating the role of FEMA Director, the Assistant Secretary has the privilege of the corresponding roles in the target-system as they relate to FEMA-oriented material. These roles can be system administrator, content examiner, publisher, and author. The ability to activate these roles is subject to the application of target-system constraints. For example, the Assistant Secretary may not activate (in S_2) both the role of content examiner and publisher simultaneously due to the constraint of separation of duties between these two system roles. Figure 9 depicts the Assistant

Secretary having activated the organizational role of FEMA Director and the system role of content examiner.

Figure 10 shows the Assistant Secretary, still using the activated organizational role of FEMA Director, activating the system role of publisher in session S_2. This activation is permitted only after the Assistant Secretary has satisfied the system constraints—in this case, by deactivating the role of content examiner. Furthermore, any additional target-system roles may be activated based on the user's organizational roles as long as they do not conflict with conditions set by system or organizational constraints.

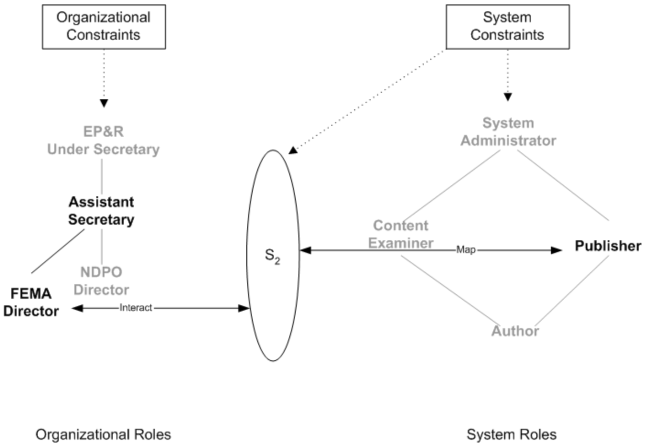

Figure 10: FEMA Director – Publisher Mapping

The Assistant Secretary may need to adjust his/her activated organizational role set (S_1) to be able to have different permissions in the target system. Continuing the same example, organizational constraints prevent the Assistant Secretary from activating the roles of FEMA Director and NDPO Director simultaneously; thus, to activate the role of NDPO Director, the Assistant Secretary must first deactivate the role of FEMA Director in session S_1. Figure 11 illustrates the Assistant Secretary having activated the organizational role of NDPO Director to act as a publisher for NDPO-related material within the DAPMS target-system.

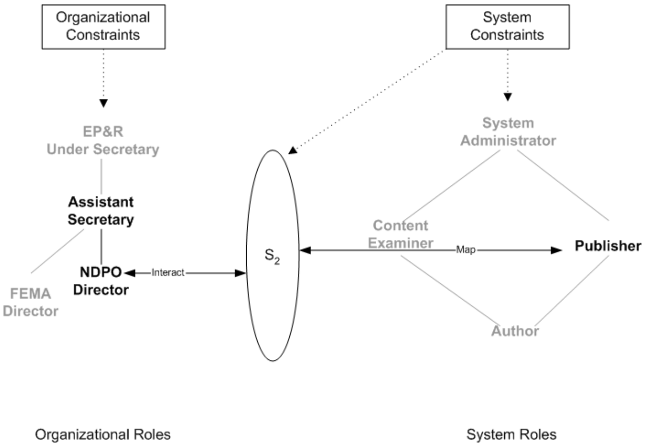

Figure 11: NDPO Director – Publisher Mapping

As described above, the constraints applied at the organizational and system levels define the roles that can be activated, as well as the permissions granted to each role. There are numerous other conditions that may be used as constraints beyond those that have been discussed; however, the intent of Figures 9-11 is to demonstrate how the application of select organizational and system constraints affects OR-SRA. These constraints are driven by the high-level security policies of the implementing organization with regards to the systems it is attempting to protect.

5. Discussion

There are several benefits of the Composite RBAC approach, the foremost of which is the explicit identification and separation of organizational and target-system roles, role hierarchies, role assignments, constraints, and role activations. This creates flexibility as well as enhanced access control granularity. According to the Composite RBAC approach, when an authority needs to delegate power either down or across the organizational role hierarchy, it does not need to cede roles in any target system other than the specific ones that it chooses. That authority could then provide as few as one role in one target system, or as many as its entire set of roles in every system (e.g., via organizational role delegation). This allows for greater flexibility in delegation for the end-user, as well as a finer level of granularity for the application of constraints. Similar to conventional RBAC approaches, system role delegation and organizational role delegation should be predicated on inherited role constraints [17].

Another key advantage of the Composite RBAC approach is that it is generic at both the organizational and target-system levels, which will allow for its adoption irrespective of the organization and the specific systems it is implemented to protect. Through introducing a two-layer abstraction, the Composite RBAC approach affords excellent scalability via the re-use of components. By separating the organizational and system role structures, these two dimensions of roles can be reused, as appropriate, to unify access control across the multitude of target systems in a large, complex organization, while also diminishing the role administration burden it faces.

Alternatively, role re-use can enable entirely different organizations to utilize the same system-level roles in their own respective target-systems despite having disparate organizational role structures. Thus, while we have proposed the Composite RBAC approach for a DAPMS at the Department of Homeland Security, it could very well be applied to other enterprise-wide systems at DHS, to individual directorates and their respective systems, or to an entirely different organization altogether. Furthermore, although our research has focused on the implementation of the Composite RBAC approach within one system and one organization, we contend that the organization-system dichotomy allows it to be applied beyond one-to-one (1:1) and one-to-many (1:n) relationships, scaling to both many organizations using one system (m:1) and many organizations using many systems (m:n). This scalable role re-use is made possible by the separation of organizational and system role hemispheres.

6. CONCLUSION AND FUTURE WORK

The foundation of the research presented here has illustrated that a new "Composite RBAC" approach can afford reusable and scaleable access controls for large, complex organizations. This contribution allows for organizational roles to be reused across various target systems within the same organization, while simultaneously enabling the re-use of target system roles across different organizations. The Composite RBAC approach adds a diverse contribution to the advancement of RBAC mechanisms and a framework for implementation in a large, complex organization such as the Department of Homeland Security (DHS). As research in this area of security grows, we acknowledge that all the concerns could not be addressed in our paper. The following are a few of these concerns that we feel are very relevant to the scope of our research.

Large, complex organizations often function in an environment of collaboration between internal and external entities; consequently, policies for access control need to be established to further define these interactions. Additionally, further studies should develop the notion of role-role assignment to incorporate the classes of enterprise roles that may exist in large organizations [10, 11]. These enterprise roles are reserved for employees engaged in enterprise-wide projects, who at times will need a variety of diverse roles associated with permissions.

Furthermore, while we present the following two methods to facilitate the activation of an organizational role, additional consideration should be given to the user's process for activating organizational roles. First, one could simply add an additional step in the user's interaction with the interface that requires the selection of an organizational role before allowing them the capabilities to perform any actions within the system. The drawback of this approach is that there is no effective way to actually enforce constraints, such as least privilege, at the behavioral level, and is therefore still vulnerable to insider threats.

Consequently, we suggest a new interaction design to address this challenge whereby a user first selects a task for a target system and is thereby automatically associated with the correct organizational and system roles. Thus, we feel the integration of task-based access control (TBAC [1]) with Composite RBAC is a crucial area of future study.

Moreover, there is a distinct need to monitor these activations to further counter the vulnerabilities from insider threats. Recently, we introduced the Composite Role-Based Monitoring (CRBM) model by extending the Composite RBAC approach to monitor insiders' behaviors, including access to resources based on their current tasks and roles within their organizations, applications, and operating systems [21]. Additional research on such insider monitoring should also be pursued in future studies.

For target-system and organizational delegation policies, a framework similar to RDM2000 proposed by L. Zhang et al. [15, 17] should be developed to take into account the new dimensions of the Composite RBAC approach that allow for both organizational and target-system roles. Additionally, research regarding cascading delegation, the delegation of delegated roles, ought to be expanded due to the increased ability to delegate without violating separation of duties and conflict of interest—a consequence of the finer granularity of the delegation capabilities afforded based on the Composite RBAC approach.

Finally, the scope of this paper primarily concerns model level issues; any actual implementation would need to take into consideration architectural issues, such as the management of each session (S_1 & S_2), as well as implementation issues like the ability to physically support multiple sessions.

7. ACKNOWLEDGMENTS

Our thanks to Dr. Ramaswamy Chandramouli at NIST (National Institute of Standards and Technology) for his useful comments.

8. REFERENCES

[1] R. K. Thomas and R. S. Sandhu. *Task-Based Authorization: A Paradigm for Flexible and Adaptable Access Control in Distributed Applications.* Proceedings of the16th NIST-NCSC National Computer Security Conference, Baltimore, MD, September 20-23, 1993.

[2] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. *Role-based Access Control Models.* IEEE Computer, 29(2): 38–47, February 1996.

[3] R. S. Sandhu, V. Bhamidipati, and Q. Munawer. *The ARBAC97 Model for Role-based Administration of Roles.* ACM Transactions on Information and System Security (TISSEC) Volume 2, Issue 1, February 1999.

[4] Z. Zhang, E. Haffner, A. Heuer, T. Engel, Ch. Meinel. *Role-based Access Control in Online Authoring and Publishing Systems vs. Document Hierarchy.* Proceedings of the 17th Annual International Conference on Computer Documentation Table of Contents, New Orleans, Louisiana, United States, October 1999.

[5] S. Osborne and G.Yuxia. *Modeling Users in Role-Based Access Control.* Proceedings of the 5th ACM Workshop on Role-based Access Control, Berlin, Germany, 2000.

[6] H. Roeckle, G. Schimpf, and R. Weidinger. *Process-oriented Approach for Role-finding to Implement Role-based Security Administration in a Large Industrial Organization.* Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, July 26-27 2000.

[7] R. S. Sandhu, D. Ferraiolo, and D. Kuhn. *The NIST Model for Role-based Access Control: Towards a United Standard.* Proceedings of the 5th ACM Workshop on Role-based Access Control, Berlin, Germany, July 26-27 2000.

[8] R.S. Sandhu. *Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way*. Proceedings of the 5th ACM Workshop on Role-Based Access Control, Berlin, Germany, July 26-27 2000.

[9] J.S. Park, R.S. Sandhu, and G.-J. Ahn. *Role-based Access Control on the Web*. ACM Transactions on Information and System Security (TISSEC), Volume 4, Number 1, February 2001.

[10] M.H. Kang, J.S. Park, and J.N. Froscher. *Access Control Mechanisms for Inter-Organization Workflow*. Proceedings of the 6th ACM Symposium on Access Control Model and Technologies (SACMAT), Chantilly, Virginia, May 3-4, 2001.

[11] J.S. Park, M.H. Kang, and J.N. Froscher. *A Secure Workflow System for Dynamic Cooperation*. Proceedings of the 16th International Conference on Information Security (IFIP/SEC 2001), Paris, France, June 11-13, 2001.

[12] R.S. Sandhu. *Future Directions in Role-Based Access Control Models.* Lecture Notes in Computer Science.

Proceedings of the International Workshop on Information Assurance in Computer Networks: Methods, Models, and Architectures for Network Security, 2001.

[13] M.P. Gallaher, A.C. O'Connor, B. Kropp. National Institute for Standards & Technology (NIST), Technology Administration. *The Economic Impact of Role-Based Access Control*, March 2002. Retrieved 11/05/03 from the World Wide Web: http://www.nist.gov/director/prog-ofc/report02-1.pdf

[14] A. Kern, M. Kuhlmann, A. Schaad, and J. Moffett. *Observations on the Role Life-Cycle in the Context of Enterprise Security Management.* Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT), Monterey, California, USA, June 2002.

[15] L. Zhang, G.-J. Ahn, and B.-T. Chu. *Applications: A Role-based Delegation Framework for Healthcare Information Systems.* Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT), Monterey, California, USA, June 2002.

[16] D. Shin, G.-J. Ahn, S. Cho, and S. Jin. *Role Engineering: On Modeling System-centric Information for Role Engineering.* Proceedings of the 8th ACM Symposium on Access Control Models and Technologies (SACMAT), Como, Italy, June 2003.

[17] L. Zhang, G.-J. Ahn, and B-T. Chu. *A Rule-Based Framework for Role-Based Delegation and Revocation.* ACM Transactions on Information and System Security (TISSEC) Volume 6, Issue 3, August 2003.

[18] Organizational Chart. U.S. Department of Homeland Security. 2003. Retrieved 10/02/03 from the World Wide Web: http://www.dhs.gov/dhspublic/interweb/assetlibrary/DHS_Org_Chart.ppt

[19] National Strategy for Homeland Security: Office of Homeland Security. 2003. Retrieved 9/30/03 from the Department of Homeland Security via the World Wide Web: http://www.dhs.gov/dhspublic

[20] What is the Mission of the New Department of Homeland Security? U.S. Department of Homeland Security. 2003. Retrieved 9/21/03 from the World Wide Web: http://www.dhs.gov/dhspublic/display?theme=10&content=429

[21] J.S. Park and S.M. Ho. *Composite Role-Based Monitoring (CRBM) for Countering Insider Threats*. 2nd Symposium on Intelligence and Security Informatics, Tucson, Arizona, June 10-11, 2004.

[22] J.S. Park and R.S. Sandhu. *Secure Cookies on the Web*. IEEE Internet Computing, Volume 4, Number 4, July-August 2000.

[23] J.S. Park and R.S. Sandhu. *RBAC on the Web by Smart Certificates*. Proceedings of the 4th ACM Workshop on Role-Based Access Control, Fairfax, Virginia, October 1999.