

Composite Role-Based Monitoring (CRBM) for Countering Insider Threats*

Joon S. Park and Shuyuan Mary Ho

School of Information Studies
Center for Science and Technology
Syracuse University
Syracuse, New York 13244-4100
{jspark, smho}@syr.edu

Abstract. Through their misuse of authorized privileges, insiders have caused great damage and loss to corporate internal information assets, especially within the Intelligence Community (IC). Intelligence management has faced increasing complexities of delegation and granular protection as more corporate entities have worked together in a dynamic collaborative environment. We have been confronted by the issue of how to share and simultaneously guard information assets from one another. Although many existing security approaches help to counter insiders' unlawful behavior, it is still found at a preliminary level. Efficiently limiting internal resources to privileged insiders remains a challenge today. In this paper we introduce the CRBM (Composite Role-Based Monitoring) approach by extending the current role-based access control (RBAC) model to overcome its limitations in countering insider threats. CRBM not only inherits the RBAC's advantages, such as scalable administration, least privilege, and separation of duties, but also provides scalable and reusable mechanisms to monitor insiders' behavior in organizations, applications, and operating systems based on insiders' current tasks.

1 Introduction

The greater an individual's knowledge of corporate internal resources, the greater the potential threat from that person. Statistically, the cost of insider threats exceeds that of outsider threats. Insiders are not interested in damaging systems or applications, but in obtaining critical information and accessing the internal level of resources. Many examples are found in government reports and news [2, 4, 5, 12, 19]. For instance, in 1985, Jonathan Pollard, who had high-level security clearance, was arrested for passing tens of thousands of pages of classified U.S. information such as satellite photographs, weapon systems data, etc., to Israelis. In 1988, a Libyan intelligence agent obtained the U.S. Military's officers' directory through his wife, who worked at the Department of Transportation and had access to the database of the Metropolitan Washington Council. In 1993, the General Accounting Office (GAO) reported that insiders' abusive use of the National Crime Information Center (NCIC) for personal

* This work was supported by the "Information Assurance for the Intelligence Community (IAIC)" program of the Advanced Research and Development Activity (ARDA).

reasons or profits had threatened the safety of U.S. citizens. In one case an NCIC terminal operator conducted an unusual amount of background search on her boyfriend's business clients. In 1998, the Social Security Administration (SSA) revealed that unethical employees had sold SSA records to a West African credit card fraud association. From the above, we certainly can see that insiders are not always friends who would benefit organizational business operation, but may be significant threats to the corporate assets.

According to the 2002 CSI/FBI Annual Computer Crime and Security Survey [12], insider misuse of authorized privileges or abuse of network access has caused great damage and loss to corporate internal information assets for many reasons, including acts of human error or failure, ignorance of top-level management, lack of enforcement of the SETA (Security Education, Training and Awareness) program with information security knowledge and awareness, ambiguous definition of policy management in a collaborative workplace, network and system vulnerabilities, an inappropriate software development control cycle that could cause an intentional or unintentional backdoor to be implanted within the systems or applications, incomplete configuration management of systems and networks, inefficient intrusion detection tools, inappropriate network infrastructural design, all-powered system administrative privileges, infrequent review of the system audit logs, and so on.

To mitigate insider threats, both technical and procedural methodologies in deterring insiders' attempts to obtain unauthorized access to internal assets in a sensitive organization, such as the Intelligence Community (IC) should be planned and deployed. Intelligence management has faced increasing complexities of delegation and granular control as more and more entities have worked together in a dynamic collaborative environment. We today are confronted by the issue of how to share and simultaneously guard information assets from one another in sensitive organizations. Many security technologies have been invented to prevent threats from outsiders, but they have limited use in countering insiders' abnormal behavior. For instance, cryptography protects information from an outsider attack trying to obtain unauthorized access to it. Signature-based network intrusion detection sensors and honeypot technology [15] monitor and log network activities, and send alerts to the administrator for early warning of flooding or denial-of-service attack. However, none of these approaches can provide an effective countermeasure against malicious insiders who already have authorized access to internal assets. Although some existing security approaches help counter insiders' unlawful behavior, they are still considered as being done at a preliminary level and efficiently prohibiting privileged insiders from internal assets remains a challenge today.

In this paper we introduce the CRBM (Composite Role-Based Monitoring) approach that is accomplished by extending the current role-based access control (RBAC [8, 11, 13]) model to overcome its limitations for countering insider threats. CRBM not only inherits RBAC's advantages such as scalable administration, least-privilege, and separation of duties, but also provides scalable and reusable mechanisms to monitor insiders' behavior, including access to resources and activities within organizations, applications, and operating systems based on insiders' current tasks. It defines a role structure in each domain and provides mappings between them. Those role map-

pings are not only horizontal (among domains at the same level; e.g., between two different organizations), but also vertical (among domains at different levels; e.g., between an organization and its applications).

We begin by identifying potential threats exploited by insiders. In particular, we provide problem analyses on insider threats to the Intelligence Community (IC). A typical scenario of how to generate intelligence reports after analyzing different sections of corporate security is given. Following this section is some related work focusing on insider threats within technical and procedural methodologies. We then describe a CRBM approach that can be used to monitor insiders' behavior based on their roles in organizations, applications, operating systems, and current tasks. We conclude by identifying plans for our future work and its possible research areas.

2 Typical Operational Scenario in IC

In this paper, we consider a scenario that fits into the typical operation of the Intelligence Community (IC). The scenario is a workflow that produces information reports and starts with the senior analyst (SA) receiving the task assignment. In the task-assignment phase, the SA decomposes the task into a number of sub-questions, which it assigns to other analysts who analyze the information requirements, collect information, analyze and produce reports, and disseminate the final reports. Individual tasks can be subdivided into a number of sub-tasks. The process involves cooperation and coordination between multiple users (insiders) with different roles spanning multiple organizations. Insiders use various applications and operating systems to fulfill their tasks. Those applications and operating systems are under different policies. Some of them are not interoperable. In the collection phase, the analyst seeks information from multiple resources that may span various organizations. It is assumed that each user must possess an organizational role in order to utilize the applications and operating systems within the IC. An analyst in a collaborative IC environment is expected to work within other roles and to become involved in different stages of the work. According to each task assignment, an analyst may need to access various areas of information.

3 Problem Analysis

Based on the above scenario we have discovered and identified three major problems in the current operation of IC: complexity, scalability, and reusability. As we explain in the following sections, we believe the CRBM approach can solve the above problems in countering insider threats by using separate role structures in organizations, applications, and operating systems, while providing mappings between them based on the insider's current task.

3.1 Complexity

In IC, there may be many users assigned to various job functions across multiple organizations. A user's *current* job functionality can be dynamically changed, based on

the context. Multiple applications and systems span multiple domains of work. For example, a junior analyst, Max, who is responsible for Project A, may not be able to gain access to other internal resources (say, of Project B) that are outside his current duties. If there are many different projects being assigned to many different insiders who belong to multiple departments within IC, there will be a complex web of assigned duties among projects, analysts, departments and/or divisions. Such a web of identities (especially with many users joining in or signing out), tasks with different status and rates of progress, and access permissions become complicated to manage and could easily cause falsely granted accessibility. For instance, the right person might not be given the right permission, or an unauthorized person could be given permission to access resources (projects) that are not part of his/her duty. Furthermore, the entire procedure is vulnerable to users' mistakes because of the complex web of users, jobs, permissions, and other constraints. For instance, a user may execute a behavior that is unrelated to his or her current task. Due to such increasing complexity in the IC, being able to control and monitor insiders' activities becomes critically important and has created huge overheads on insider threat monitoring.

3.2 Scalability

A common phenomenon in the IC is that people join in and sign out of jobs frequently, based on their current task. For example, Bob is responsible for ten projects as a senior analyst in the IC. If, one day, Bob resigns from the IC, John has to come in to partially take over what Bob previously worked on, say five projects. Alice, a junior analyst, is assigned to work on two of those tasks that Bob has left. Thomas, a director, may come in to work on the three tasks that are about to be delivered to the customer. Those ten projects were supposed to be finished by Bob alone if he were still with the IC; however, ten projects now have to be split into three groups owned and supervised by three different personnel within the IC. Obviously, we need a more scalable management in this case. Furthermore, changing one user's permissions for the distributed resources is very tricky in the conventional identity-based approach (e.g., there may be permission revocation from many different files that are distributed in various places) because of the direct mapping of identity and permission. Typically, therefore, a system administrator cancels a resigned user's account or changes the user's passwords for this purpose, which implies that the identity-based approach (revocation in the example) is not reliable. In order to strengthen the competitiveness of the IC so that it provides the best quality of service, it has to overcome the scalability problem when there is a dilemma concerning the management of identities, permissions, controlling the accessibility of the resources, and providing other constraints.

3.3 Reusability

Whenever there are multiple applications and systems used within an organization in order to counter insider threats, there is a need to provide effective and powerful monitoring mechanisms for each and every single domain (e.g., various applications

and systems) that is being used in the organization. However, we must assume that the organization will update or change some of those applications or systems in the future. If we had to modify each monitoring mechanism or strategy whenever we change a system or an application, it would be too costly and complex, which could cause technical or procedural errors in monitoring. This obviously does not fit into the IC operational environment, where many applications are dynamically installed and uninstalled, and systems are frequently added to or removed from the domain. Furthermore, an entire organization may join or leave the community with its own applications and systems. Hence, there is a pressing need for a reusable monitoring mechanism for each domain that can be easily integrated with other domains. In other words, if each application, system, or even organization has its own monitoring structure with a well-defined interface, we can simply integrate it with others.

4 Management vs. Technology for Countering Insider Threats

We briefly describe what some other scholars had in mind regarding insider threats. Although various aspects such as policy administration, SETA, and detective and preventative technology have been discussed, we divide this topic into management and technology viewpoints.

4.1 Management Approaches

Peter Neumann states that a large percentage of threats are caused by insiders' misuse of information and by privileges being improperly authorized [6]. Even audit trails are inadequate to monitor unauthorized access because privileged insiders have the potential to compromise systems. Some risks to insider threats are identified as (1) no fine-grained access control system is implemented, (2) all-powerful administrator root privileges are given, and (3) no serious authentication mechanism is practiced. Techniques such as separation of duties, split-key encryption, and enlightened management are urgently required to implement and guard corporate information security.

Whitman has pointed out the top 12 information security threats named in the CSI/FBI Annual Computer Crime and Security Survey and compared the 2002 statistics with those of 2001 [12, 19]. The comparison identified an increasing awareness of insider threats. From the statistics, the threat of "insiders' abuse of net access" ranked in second place in 2001 and continued to rank second in 2002. The threat of "unauthorized access by insiders" ranked in fourth place in both 2001 and 2002. In addition, Whitman identified 12 categories of new threats from a survey. Among these, the top six threats are all related to unethical human behavior such as human error or failure, intellectual property violation, deliberate acts of espionage or trespass, information extortion, sabotage or vandalism, and theft. From such identification, Whitman has indicated that a consistent security policy and ethical training are critical to the prevention of malicious insider acts. Unfortunately, neither the information security policy nor ethical training is being practiced by the corporation as protection mechanisms. Thus, Whitman promotes the importance of the SETA (security education, training, and awareness) program because any security profile begins with a valid security

policy. Such policy is then translated into action through an effective security plan that focuses on the prevention, detection, and correction of threats.

Quigley has shown how dangerous it can be for ex-employees who, out of greediness and revengefulness, hack into a corporate internal network [17]. Many businesses have moved toward a collaborative setup with downstream distributors and resellers, and therefore upstream vendors and suppliers, employee screening, interviewing and background checking have become vitally important to the prevention of insider sabotage incidents. Not only because of the employee's ethics issue, a company itself also has to maintain an upscale secure operation because ex-employees are often allowed to continue to access the company's internal resources, database, file servers, intranets and email, along with their remote access to VPN and dial-in accounts. Such "back doors" to the corporate network should be thoroughly examined and restricted. Network monitoring services have gradually become popular as more and more businesses are willing to hire professional companies to monitor their business networks and catch saboteurs. An emphasis on information security from different management angles such as laws and regulations, network monitoring services, risk assessment, and cyber insurance practices has become substantial for countering insider threats.

4.2 Technical Approaches

As a technical countermeasure at the network level, Vetter, Wang, and Wu have mentioned that providing security in a routing protocol must involve the protection of authenticity and integrity of routing protocol messages [18]. There has been a consideration of using cryptography; however, it comes to a performance trade-off when the encrypting and decrypting packets dramatically slow down the network transmission rate. Even if the cryptographic authentication does prevent forging, replay, and modification of protocol messages by outsiders, the threat still exists when an intruder is able to block or delete messages transmitted on the link. Regarding the internal threats, it is still not practical to use conventional cryptographic solutions since there is a need for a pair of routers to share a secret key. The insider here is defined as a protocol participant; any router that exchanges routing information internally is viewed as the insider. The authors mentioned that the OSPF (their proposed routing protocol) does provide some inherent protections. For example, bad information flooded into one area does not affect routing in other areas. Several routers that have access to the same set of information do check each other for corroboration.

Honeypot technology is an approach that has been used to detect and decoy outsider threats deployed at the perimeter network and now can be used to identify, trace and gather information related to insider threats [15]. Since honeypots collect much smaller data sets compared to the millions of logs and thousands of alerts generated by traditional technology, they reduce false positives compared to the anomaly-based IDS technologies, and catch false negatives that could not be detected by traditional signature-based IDS. Honeypot creates a trap, a disguised environment to entice illegal users and their improper and unlawful behavior. Not only honeypots can trace and gather information for forensics. Spitzner has also mentioned that honeytokens could work as digital entities that lure intentional insiders to the honeypots [15]. Spitzner has

specified that simply deploying honeypots on the internal network would not be likely to detect advanced insiders, since most of them would already have proper privileges to such critical resources. The strategy here is to use thousands of honeypots as small as honeytokens, instead of just one, to interact with attackers. This would dramatically increase the likelihood of capturing attackers.

There are many other technical approaches to monitoring insider threats [1, 7]; however, none of those approaches as yet provide a comprehensive solution to IC.

5 The CRBM (Composite Role-Based Monitoring) Approach

5.1 Role-Based Access Control (RBAC)

RBAC has rapidly emerged in the 1990s as a technology for managing and enforcing security in large-scale enterprise-wide systems. The basic notion of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles, thereby acquiring the roles' permissions. Figure 1 shows a simplified RBAC model. RBAC ensures that only authorized users are given access to certain data or resources. From the initial conceptions of RBAC, a family of RBAC models (RBAC'96 Model) was developed in 1996 by Ravi Sandhu and associates [14]. This model was in turn adapted to be the NIST unified standard RBAC model in 2000 [3]. 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, 10, 11].

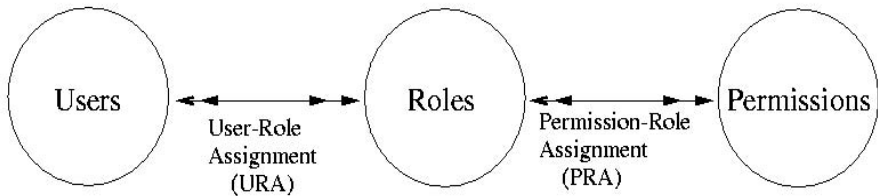


Fig. 1. A Simplified RBAC Model

In RBAC, a role is a semantic construct forming the basis of an access control policy. System administrators can create roles, grant permissions to those roles, and then assign users to the roles on the basis of their specific job responsibilities and policy. RBAC provides the mapping between users and permissions through User-Role Assignment (URA) and Permission-Role Assignment (PRA). Usually, PRA is more stable (of course, it can be changed if necessary) than URA, because job responsibilities in an organization do not change frequently, while users' job functions change quite often. The system makes access control decisions based on the users' roles instead of their identities. This provides an efficient access control mechanism to the system and resolves the scalability problem.

5.2 RBAC Enhancements for CRBM

Although many researchers have suggested various ways to prevent insider threats, most of those approaches have been limited to applying within a single domain or between domains at the same level (e.g., between organizations or between systems, not between an organization and a system). The reality is that an organization is not only composed of a single domain, but has become a collection of different domains (including organizations, applications, and operating systems) out of the business inter-cooperativeness in nature. Thus, in order to provide a robust and comprehensive monitoring mechanism for countering insider threats, we introduce the CRBM approach, which would map out the authorization in one domain with another vertically (such as role mappings among domains of systems, applications and organizations) as well as horizontally (such as role mappings among different organizations). This approach maps out the roles among various domains in a concrete authorization and monitoring system.

The CRBM approach is based on the extended concepts of RBAC. We still provide the inherent benefits of the role-based approach, but we would like to discuss the limitations of the original RBAC that are enhanced for CRBM.

- 1) RBAC was originally designed for strong, effective, and scalable access control. It provides scalable administration, least privilege, and separation of duties to the target domain for its access control. However, the scope of insider threats is broader than that of access control. Access control is a critical component for countering insider threats, but we also need to monitor other insider behavior such as communication patterns, frequencies, areas of topics, areas or interests, etc. Therefore, CRBM provides a comprehensive behavior-monitoring mechanism based on the insider's roles in organizations, applications, and operating systems, where each role is assigned to a set of expected or unexpected behaviors that include not only access to assets but also others.
- 2) Insiders normally would already have some level of privileges over the resources within domains such as organization, applications, and systems. An access control mechanism, although much more effective than firewall technology and with the ability to provide fine-granted control within the use of the applications and systems of organizations, cannot provide full security control to privileged insiders and thus is not sufficient to counter an insider's misuse of information. Suppose a malicious system administrator, Bob, were to arbitrarily release users' ids, passwords, SSNs or contact information to his external partners, his action would infringe upon the current access control mechanisms. An insider's misbehavior cannot be detected by the RBAC approach or any other security mechanisms if the insider is a privileged user. Obviously, Bob has abused his privileges in the example, but with current access control or monitoring technology, such behavior cannot be monitored or detected because most security models and mechanisms, including RBAC, are designed to detect unauthorized users' abnormal access. Once users are granted privileges, they are lawful and powerful insiders, and their misbehavior is not monitored at all. Therefore, by comparing the insider's actual behavior and the set of expected or unexpected behavior defined, based on the in-

sider's roles and current work, CRBM provides stronger and more accurate monitoring mechanisms than those of existing approaches for the purpose of countering insider threats.

- 3) In the original RBAC approach, a user (insider with granted privileges, in our case) can choose one or more roles (among his or her assigned roles) that he or she is going to use in the session (known as a set of activated roles in RBAC). RBAC would offer least privilege via using the concept of the session in order to make systems more secure. However, the RBAC approach assumes and trusts that the privileged user always activates necessary roles in a particular session for specific tasks. Still, once the user is granted certain privileges, there is basically no mechanism to control behavior as being rightful or not. Say a user, Alice, is assigned to Administrator, Analyst, and Employee roles, and her current task is to generate a survey report that requires the Analyst role. It is the most reasonable behavior if Alice activates the Analyst role and uses the role's corresponding privileges. However, she could activate the Administrator role as well as the Analyst role in the same session and misuse her privileges (e.g., change the system configuration files with the permission associated with the Administrator role). The concept of a session in current RBAC approaches can be exploited by insiders to misuse their privileges. Thus, CRBM provides the mappings between the sessions of organizational, application, and operating systems roles. These mappings can be dynamically changed based on the user's current task, which can prevent an insider from abusing his or her roles across the domains.
- 4) RBAC approaches typically consider the role structures within a single domain or multi-domains at the same horizontal level (e.g., between organizations or between systems). The abstraction of the role structure for a single domain is certainly simple and of great benefit, but it does not provide the essential explicitness of a complicated inter-related organizational or system structure. In order to make the abstraction of the role structure more applicable to multiple domains so that it can counter insider threat effectively in a reusable manner, the need is pressing to consider role structures among multi-domains at different levels (e.g., between an organization and a system) as well as at the same level. This makes the current role-based approaches much more scalable, effective, and reusable. CRBM satisfies these requirements by separating the role structures of organizations, applications, and operating systems, and by providing mappings between them. Those role mappings are not only horizontal (among domains at the same level) but also vertical (among domains at different levels).

5.3 CRBM Architecture

Figure 2 depicts the CRBM architecture used to monitor the behavior of an insider (Alice). In summary, the behavior of the insider is being monitored in the organization to which she belongs, in the software application she is using, and in the operating system of Alice's machine. All of Alice's monitored behavior in those domains is analyzed based on her current task [16] and roles in order to detect if she has misused her privileges.

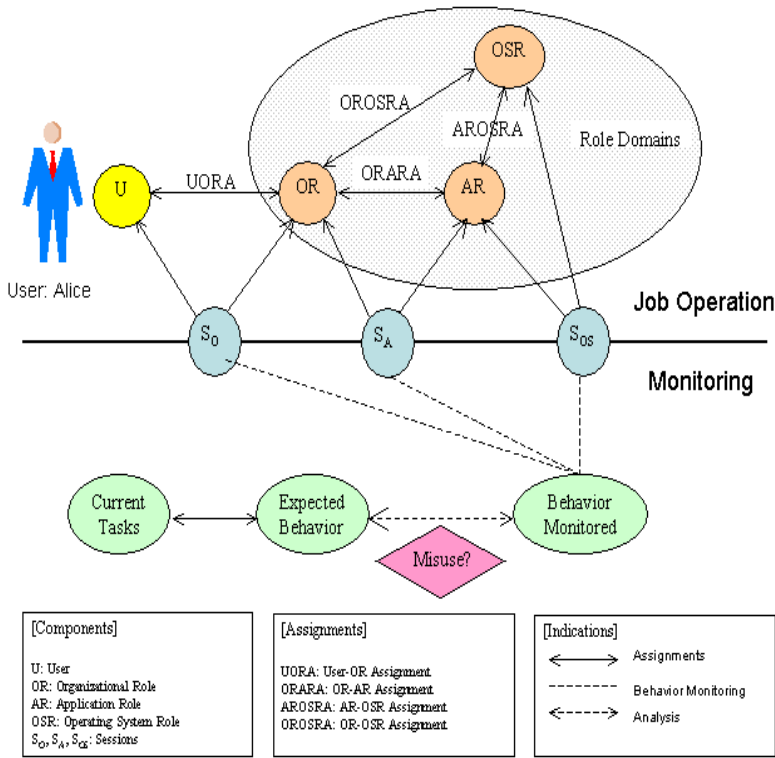


Fig. 2. CRBM Approach

The CRBM approach to monitoring insider threats maps role structures into three independent domains: organization role (OR), application role (AR), and operating system role (OSR). OR depicts the roles defined at the organization level. Likewise, AR depicts the roles defined in the application and OSR in the operating system. We assume that a user (U) is assigned to organizational roles before the operation by the global policy to perform his/her duties. S depicts a session, which is a set of activated roles. In the figure, for example, the S_0 is the set of organization roles activated by Alice. S_A is the set of application roles activated for Alice, and S_s is the set of OS roles activated for Alice. OR are assigned to the insider's identity (e.g., OR Employee is assigned to Alice), while AR and OSR are assigned to the corresponding OR (not the insider's identity directly). For instance, AR Reader can be assigned to OR Employee, not to Alice. As a result, Alice has AR Reader in the application because she is an employee of the organization, not because she is Alice. Typically, to use an application or a system in an organization, the user should first be assigned to some organizational roles such as Employee. Likewise, OSR is assigned to AR, which allows the user to run the applications in the operation systems, based on the user's OR. If a user's current task requires direct access to the OS (not through any applications—but,

for instance—file management in the user’s machine), we need to provide a direct mapping between OR and OSR.

Users in an organization are commensurate with their job functions as well as with their positions within the organizational role structure (e.g., role hierarchy). The process of assigning users to organizational roles is called user-OR-assignment (UORA). Likewise, target applications and operating systems may have independent role structures (AR and OSR, respectively). OR and AR are bridged by the OR-AR-assignment (ORARA). We believe each application should have its own role structure that is independent of other domains in order to provide more scalable and reusable monitoring mechanisms. As with application roles, each OS has its own role structure. This creates an OS role structure (OSR) in the figure. AR and OSR are bridged by AR-OSR-assignment (AROSRA). The role structure from each domain can be used as a monitoring interface for that domain when one role structure is integrated with others. Likewise, OR and OSR are bridged by OR-OSR-assignment (OROSRA), which increases the reusability of the monitoring mechanism. The assignments among users, organizational roles, application roles, operating system roles, and their sessions have effectively formed a scalable and reusable net to monitor insiders’ behavior.

The user activates the sessions (the organizational session is usually activated first, which triggers the activation of other sessions manually or automatically). Based on her current task in the domains, she is allowed to use the corresponding privileges in the domains. A detailed description of the session activations and their interdependencies are found in [8]. In CRBM, the user’s behavior in three different sessions (organization, application, and OS) are monitored. Finally, the monitored behavior is compared with the expected or unexpected behavior, which is defined based on the user’s current task, to find out if the user misused her privileges. For instance, let us say that an authorized user (insider), Alice, is assigned to organizational roles (OR) such as Employee, Analyst, and Administrator, and her current task is to generate a survey report, which requires the Analyst role. Suppose Alice activates the Administrator role as well as the Analyst in the same session (S_o), which automatically generates the corresponding S_A and S_{os} , and misuses her administrative privileges while finishing her current task (e.g., she changes some sensitive configuration files in the system). This situation can be detected by CRBM if the insider’s behavior (i.e., changing the system configuration) is not defined in the current task’s expected behavior set. This can work even when the insider abuses her privileges under her current task. In the example, Alice activates just the Analyst role, which is required for her current task, makes a copy of sensitive information, and emails it to her external partner. This behavior can also be detected by CRBM by comparing Alice’s behavior in S_A and S_{os} with the set of expected and unexpected behavior that were defined based on the policies.

6 Conclusions and Future Work

In this paper we identified the generic problems for countering insiders’ behaviors in IC with respect to complexity, scalability, and reusability. After coming to an under-

standing about how other scholars have analyzed threats by advanced insiders at both management and technical levels, we introduced our CRBM approach by extending existing RBAC approaches with separate role structures of organizations, applications, and operating systems, and mappings among them. We explained each component that participates in the correlation of role domains and how the mappings of role structure and activation of sessions have come into the picture.

In our future work, we will attempt to apply the CRBM approach to a real IC scenario and we hope to shape our approach into a firm model. By using the delegation monitoring mechanism, we should be able to monitor users' behavior and identify users' improper intension on the internal network according to their delegated roles. We will also attempt to apply this approach to monitoring the all-powerful system administrators' activities. Possible integration with other technologies such as firewalls, intrusion detection systems, and the application of honeypot/honeytoken decoying technologies for monitoring insider threats will be further considered.

Acknowledgments

The authors are grateful to Eric Brown, Bob Delzoppo, Matt Downey, Liaquat Hos-sain, Elizabeth Liddy, Anand Natarajan, and Svetlana Symonenko for their useful discussions and comments.

References

1. Robert H. Anderson, Thomas Bozek, Tom Longstaff, Wayne Meitzler, Michael Skroch, Ken Van Wyk. *Research on Mitigating the Insider Threat to Information Systems - #2: Proceedings of a Workshop Held, August 2000.* <http://www.rand.org/publications/CF/CF163>.
2. Dorian Benkoil, *An Unrepentant Spy: Jonathan Pollard Serving a Life Sentence.* ABCNEWS.com Oct. 25, 1998.
3. David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli, *Proposed NIST Standard for Role-Based Access Control.* ACM Transactions on Information and System Security (TISSEC), Vol. 4, No. 3, August 2001, Pages 224–274.
4. Michale V. Hayden. *The Insider Threat to U. S. Government Information Systems.* National Security Telecommunications and Information Systems Security Committee (NSTISSAM) INFOSEC 1-99, July 1999. http://www.nstissc.gov/Assets/pdf/NSTISSAM_INFOSEC1-99.pdf
5. Jacob V. Lamar Jr. *Two Not-So-Perfect Spies; Ronald Pelton is Convicted of Espionage as Jonathan Pollard Pleads Guilty.* Time 16 June, 1986.
6. Peter G. Neumann. *Risks of Insiders.* Communications of the ACM, Volume 42, Issue 12, December 1999. ISSN: 0001-0782.
7. Nam Nguyen, Peter Reiher, and Geoffrey H. Kuenning, *Detecting Insider Threats by Monitoring System Call Activity.* Proceedings of the IEEE Workshop on Information Assurance, West Point, NY June 2001.

8. Joon S. Park, Keith P. Costello, Teresa M. Neven, and Josh A. Diosomito. *A Composite RBAC Approach for Large, Complex Organizations*. 9th ACM Symposium on Access Control Models and Technologies (SACMAT), Yorktown Heights, New York, June 2-4, 2004.
9. Joon S. Park, Ravi Sandhu, and SreeLatha Ghanta. *RBAC on the Web by Secure Cookies*. 13th IFIP WG 11.3 Working Conference on Database Security, Seattle, Washington, July 26-28, 1999.
10. Joon S. Park and Ravi Sandhu. *Secure Cookies on the Web*. IEEE Internet Computing, July-August 2000.
11. Joon S. Park, Ravi Sandhu, and Gail-Joon Ahn. *Role-Based Access Control on the Web*. ACM Transactions on Information and System Security (TISSEC), Volume 4, Number 1, February 2001.
12. Richard Power. *CSI/FBI Computer Crime and Security Survey*. Computer Security Issues & Trends, 2002.
13. Ravi S Sandhu, Edward J Coyne, Hal I. Feinstein and Charles E. Youman, *Role-Based Access Control Models*. IEEE Computer, Volume 29, Number 2, February 1996.
14. Ravi Sandhu, David Ferraiolo and Richard Kuhn. *The NIST model for Role Based Access Control: Towards A unified standard, Proceedings*. Proceedings of the 5th ACM Workshop on Role Based Access Control, July 26-27, 2000.
15. Lance Spitzner. *Honeypots: Catching the Insider Threat*. Proceedings of the 19th Annual-Computer Security Applications Conference, 2003.
16. Roshan K. Thomas and Ravi Sandhu. *Conceptual Foundations for a Model of Task-based Authorizations*. In Proceedings of the IEEE Computer Security Foundations Workshop (CSFW), Franconia, New Hampshire, June 1994.
17. Ann Quigley. *Inside Job*. netWorker, Volume 6, Issue 1, Pages: 20 – 24, March 2002. ISSN: 1091-3556.
18. Brain Vetter, Feiyi, S. Felix Wu. *An Experimental Study of Insider Attacks for OSPF Routing Protocol*. IEEE International Conference on Network Protocols, pp. 293 - 300, October 1997.
19. Michael E. Whitman. *Enemy at the Gate: Threats to Information Security*. Communications of the ACM, Vol. 46, No. 8., August 2003.