Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Activity Theory Guided Role Engineering

Manish Gupta
SUNY Buffalo, mgupta3@buffalo.edu

Activity Theory Guided Role Engineering

Manish Gupta
State University of New York, Buffalo
mgupta3@buffalo.edu

ABSTRACT

Roles are convenient and powerful concept for facilitating access to distributed systems and enforcing access management polices. RBAC is one the most widely used role engineering models in enterprises. Several threats arise due to insecure and inefficient design of roles when social and interaction dynamics in an organizational setting are ignored. Activity theory is one of the most applied and researched theories in context of understanding human actions, interactions with environments and dynamics against different social entities. The paper, first, presents overview of role-engineering and activity theory. Then the paper presents different methods in which activity theory can be applied for efficient and secure role-engineering processes. A case study, carried out at a US-based midsize financial institution, is also presented to demonstrate 1) how traditional role-engineering processes give way to threats and 2) how using activity theory models (2 used in this paper) can mitigate risks in role-engineering process.

Keywords: Activity Theory, Role engineering, Risk Management, RBAC, case study

INTRODUCTION

Roles are convenient and powerful concept for facilitating access to distributed systems and enforcing access management polices. Although the concept of a role has been used by researchers (Biddle and Thomas, 1979; Ferraiolo and Kuhn, 1992; Schaad at. Al, 2001) for many years, the establishment of the RBAC96 model (Sandhu et al, 1996) and subsequent variants of the RBAC models have provided the most impetus to the research area of access control models. Many organizations are moving to role based access control. The process of developing an RBAC structure for an organization has become known as "role engineering". Role engineering can be a complex undertaking. For example, in implementing RBAC for a large European bank with over 50,000 employees and 1,400 branches serving more than 6 million customers, approximately 1,300 roles were discovered (RBAC Standard, 2008). Role engineering originated from the need to create a set of roles that encapsulates the functionalities and responsibilities of a working enterprise (Coyne, 1995). The intuitive method of identifying roles is by elicitation; extraction from job functionalities, scenarios and processes (Neumann and Strembeck, 2002; Roeckle et al, 2000).

Activity Theory seeks to explain social and cultural work practices by relating them to the cultural and historic context in which the work activity, which is the basic unit for analysis, is taking place. Using activity theory, user needs are understood both historically and as something to be constructed collaboratively. Activity theory shares the idea, with other contemporary theories, that a hierarchical analysis of human action is valuable with means and ends analysis, task analysis alike (Bertelsen and Bodkaer, 2003). Thus the conceptual framework of Activity theory has been seen as a way of providing a means of analyzing the actions and interactions with artifacts within a historical and cultural context (Rogers, 2004). Activity Theory is thus seen as being useful to design interfaces and systems that take into account the context of use and thus can play an important role in better user experiences. Activity theory has been used for a framework to enhance the business value of a firm's resources. Given the unique offerings of activity theory, it can be successfully applied for understanding users, roles and privileges to design secure role-engineering processes.

The paper is organized as follows: Next Section presents background and motivation for this paper, specifically why Activity theory is used to guide role-engineering tasks. Section on preliminaries presents concepts and definitions in form of preliminaries that are needed to understand the role engineering process when analyzed using principles and concepts of activity theory. Section on Activity Guided Role Engineering presents overview of RBAC model adapted to include activity theory's system components and Activity theory model adapted to show RBAC components. Following Section presents a real-world analysis of role engineering process from an activity theory perspective. This example is based on information gathered through semi-structured interviews and round table discussions conducted with 2 application managers and 4 information security specialists at a mid-sized US-based financial institution. The paper concludes with conclusions and brief discussion on future work.

BACKGROUND AND MOTIVATION

Activity theory offers the options for understanding use and system design for computer applications as well as other parts of the work activity are constantly reconstructed to meet the dynamic demands of any organization. An explicit awareness of these hidden trends may change our way of doing design (Floyd, 1987). Researchers (Mwanza 2001; Korpela, Soriyan et al., 2000) have proposed AT-based methodologies for software development. Several other disciplines have used Activity Theory to understand their processes and constructs. However, note that due to origins and wide applications of it in social and psychological areas, activity theory is vastly under utilized in information security areas.

As is evident from the literature review that role engineering is an increasingly critical and vital process at any organization from both functionality and security viewpoints. It is also revealed through literature review that activity theory has not been used, thus far, to analyze and understand role-engineering process to design effective and secure roles within an organization. With Activity theory's immense benefits, I analyze role-engineering process and principles to unravel some of the human and social facets that are not evident from traditional role engineering frameworks.

PRELIMINARIES

RBAC

With continuously growing numbers of applications, enterprises face the problem of efficiently managing the assignment of access permissions to their users. In an information system, data protection against improper disclosure or modification is an important requirement. The access control regulates what a user can do directly and what the programs executed on behalf of the user is allowed to do. There are standard models (RBAC96 (Sandhu et al, 1996), NIST2001 (IT 2004)) and active research on its extensions (Sandhu et al, 1996, Sandhu et al, 1997; Kern 2002). Figure 1 shows Sanshu's RBAC96. Since the early 1990s, Role-Based Access Control has become more popular, which is an interesting alternative to the traditional access-control models, like MAC (Mandatory Access Control) or DAC (Discretionary Access Control) (Ferraiolo and Kuhn, 1992). Mainly enterprises with many users and high security demands like banking companies are now considering RBAC and role concepts, and therefore facing the problem of how to define roles. Role-based access control (RBAC) has been adopted successfully by a variety of commercial systems. As a result, RBAC has become the norm in many of today's organizations for enforcing security. Basically, a role is nothing but a set of permissions. Roles represent organizational agents that perform certain job functions within the organization. Users, in turn, are assigned appropriate roles based on their qualifications (Sandhu et al, 1996, Ferraiolo et al, 2001). However, one of the major challenges in implementing RBAC is to define a complete and correct set of roles. This process, known as role engineering *(*Coyne, 1995), has been identified as one of the costliest components in realizing RBAC (Gallagher , 2002).

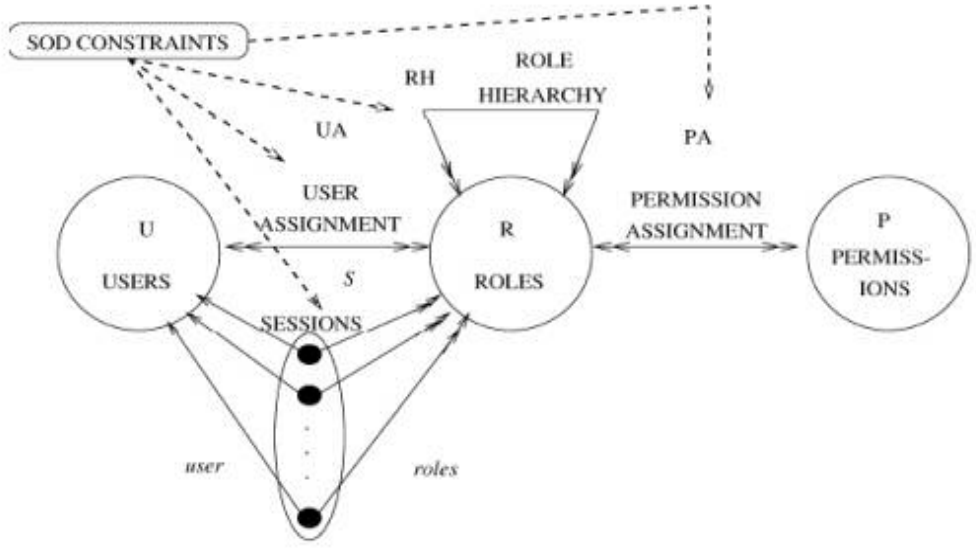

Figure 1. RBAC96 (Sandhu et. al, 1996)

Role Engineering

Role engineering originated from the need to create a set of roles that encapsulates the functionalities and responsibilities of a working enterprise (Coyne, 1995). Essentially, role engineering is the process of defining roles and assigning permissions to them. Role engineering for role-based access control (RBAC) is the process of defining roles, permissions, constraints and role-hierarchies (Coyne, 1996). The intuitive method of identifying roles is by elicitation; extraction from job functionalities, scenarios and processes (Neumann and Strembeck, 2002; Roeckle et al, 2000). Initial approaches used use cases to group actions performed in a particular procedure into a role (Fernandez and Hawkins, 1997). The definition of a role concept (role engineering) is a difficult task traditionally performed via interviews and workshops. Role engineering is a tedious, error-prone and politically difficult task. Once role definitions are established, there is latency and efforts to gain more privileges per job demands. So, people are hesitant to specify roles and reluctant to co-operate.

There are generally two approaches to role engineering (Epstein and Sandhu, 2001): Either working top-down from an initial description to roles and permissions or else aggregating permissions bottom-up into roles. The first approach starts with business process definitions or scenarios, extracts role candidates from these descriptions, and then transforms them into an enterprise role concept (Roeckle, 2000; Roeckle et al, 2000). The roles are then fitted with the necessary permissions. This approach is time-consuming and error-prone. It also requires early co-operation of employees and/or experts and is harder to support with a tool: the necessary knowledge is in people's minds and has to be externalized first. The second approach starts bottom-up by analyzing artifacts of roles (Kuhlmann et al, 2003) and then transforms and aggregates them into the roles themselves. The idea here is that roles are already implicitly in use (Sandhu et al, 1996) and have to be identified rather than defined. Therefore, relying solely on a top-down approach in most cases is not viable, although some case studies (Schaad et al, 2001) indicate that it has been done successfully by some organizations (though at a high cost). In contrast, since organizations do not exist in a vacuum, the bottom-up approach utilizes the existing permission assignments to formulate roles. Starting from the existing permissions before RBAC is implemented, the bottom-up approach aggregates these into roles. It may also be advantageous to use a mixture of the top-down and the bottom- up approaches to conduct role engineering. While the top-down model is likely to ignore the existing permissions, a bottom-up model may not consider business functions of an organization (Kern et al, 2002). However, the bottom-up approach excels in the fact that much of the role engineering process can be automated. Role mining can be used as a tool, in conjunction with a top-down approach, to identify potential or candidate roles which can then be examined to determine if they are appropriate given existing functions and business processes.

Role: Concept and Issues

Roles can be differentiated between functional and organizational roles. Functional roles are based on business functions within a company. Organizational roles correspond to the hierarchical organization in a company in terms of internal structures. Functional roles, in contrast to organizational roles, are robust against organizational restructuring since business tasks are often not embedded in organizational structures. The research of roles to set up in an organization is a complex task because of poor formalization of functional roles. Often, this is a cooperative process where various authorities from different disciplines understand the semantics of business processes of one another and then incorporate them in the form of roles. Since there could be often dozens of business processes, tens of thousands of users and millions of authorizations, this is rather a difficult task. Moreover, the role concept is an abstract approach and does not tune with physical entity or object. Role engineering has been defined as the process of defining roles, permissions, role hierarchies, constraints and assigning the permissions to the roles (Coyne, 1996). In order to explain the determination of roles and/or the research of their associated permissions, many concepts were proposed. Fernandez and Hawkins (1997) used the''use case" formalism to define the permissions associated to a given role. Thomsen et al. (1998) proposed the RBAC-FNE model (Role-Based Access Control Framework for Network Enterprises) based on seven layers that may be exploited by various users (i.e. application developer or system administrator). In his approach, Epstein and Sandhu (2001) proposed to determine the roles and their associated permissions starting from an extension of the RBAC model which includes three new concepts between roles and permissions: jobs, work patterns and tasks. Neumann and Strembeck (2002) proposed to determine functional roles (and their associated permissions) of an enterprise starting from the scenarios, where each role is depicted using a collection of scenarios and each scenario is associated with a set of particular access operations. He and Antn (2003) describe a goal-driven role engineering process.

Activity Theory

Activity theory originated from the works of several Russian scholars. Vygotsky adapted Marx's political theory regarding collective exchanges and material production to capture the co-evolutionary process individuals encounter with their environment while learning to engage in shared activities (Stetsenko, 2005). Activity theory has evolved through 2 more generations of research (Engeström 1999). The second generation overcame the limitation of Vygotsky's work which was that the unit of analysis remained individually focused. The third generation was popularized by Engeström (1999), which is concerned with the process of social transformation and incorporates the structure of the social world and aims to understand dialogues, multiple perspectives and networks of interacting activity systems.

Activity Theory provides a set of basic principles to capture a broader conceptual framework with which to understand the goal oriented, socially and culturally influenced work practices of humans using computers. Human activities are driven by human needs in order to achieve certain purposes. The activity in question is usually mediated by tools and this concept of mediation of activity using artifacts is a central theme of this theory. Most of human activities are collective ones taking place in rich communal and social environments. A systemic model (Figure 3), proposed by Engeström (1987), is used to explain collective activities and cooperative work. An activity is undertaken by a human agent (subject) who is motivated toward the solution of a problem or purpose (object), and mediated by tools (artifacts) in collaboration with others (community). The structure of the activity is shaped and constrained by cultural factors including conventions (rules) and social divisions (division of labor) within the context.

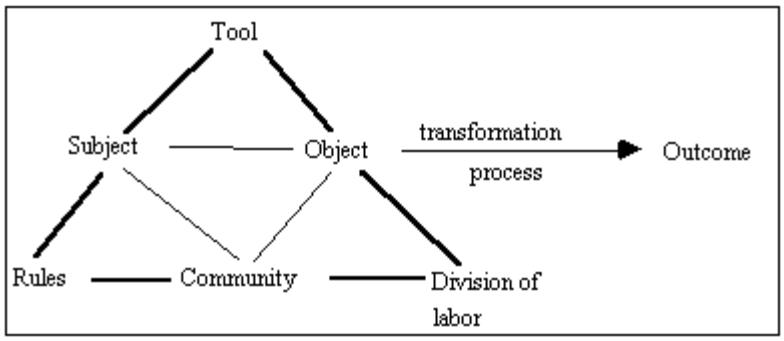

Figure 2. Engestrom's extended Activity System Model. (1997)

In Engestrom's original work, activity systems included subject, tool, object, rules, community, distribution of labor, and outcomes as shown in Figure 2. **Subjects** are participants of activity and tools are resources that subjects use to obtain the object or the goal. **Rules** can be informal or formal regulations that subjects need to follow while engaging in the activity. The **community** is group that subjects belong to and **division of labor** is the shared responsibilities determined by the community. Any component of an activity system can bring about tension in the subject's effort to attain the object. Finally, the **outcome** is the consequence that the subject faces as a result of the activity. Activity systems analysis was developed to explore and document the sources of tensions in human individual or collective activities. Engestrom (1987) originally introduced his model as a tool for participants to understand the complex psychological phenomenon involved in their activities and facilitate an iterative learning process. His intention was to help participants identify tensions in their practices and develop strategies to overcome them.

ACTIVITY THEORY GUIDED ROLE ENGINEERING

Activity theory (AT) has its roots in the cultural–historical psychology. It provides a systematic and yet practical framework for analyzing work activities and their complex intrinsic relations (Korpela et al, 2002; Engestrom and Miettinen, 1999). In AT, the object of analysis is the whole activity system. Single actions relating to a certain organization, occupation, individual, or tasks are just a part of the environment in which the overall activity takes place. This clearly distinguishes the AT approach from "traditional" process modeling. One individual usually performs an action, whereas the reason for an activity to exist is to achieve something that requires a collective. Division of work, mutual rules and various means of communication coordinate actors and their actions. The actions need to be directed towards the shared object and the desired outcome, although the actors do not necessarily represent the same organizations and actors may even be unaware of each other or of their own role in the system (Korpela et al, 2002; Engestrom, 1987). Similar to all systemic entities, activity systems have internal and external interactions. Rules, actors, tools, and objects of an activity system are received from various other activity systems. In AT, activity is seen as a systemic entity, i.e. there must be a relative correspondence between the activity as a whole and its elements. Further, they have a strong role as a means of coordination and communication within the activity system (Korpela et al, 2002;Kutti, 1991; Engestrom, 1987). Thus, ICTs are intertwined with the very essence of the work itself (Kutti, 1991). It is understandable that ICT has such a fundamental impact on work. Using these basic tenets of activity theory, I next propose adapted models for analyzing and understanding role engineering.

Activity Theory with RBAC

I analyzed Engestrom's extended Activity System Model and RBAC model (Sandhu et al, 1996) and observed similarities between the two. Below I present Engestrom's model showing different components and processes of RBAC model. The items in italics and within parentheses are different components of RBAC that I consider while designing roles. They are presented next to activity theory components that they relate to. While engineering roles using activity theory the system components in box should be used to uncover RBAC components in parentheses.

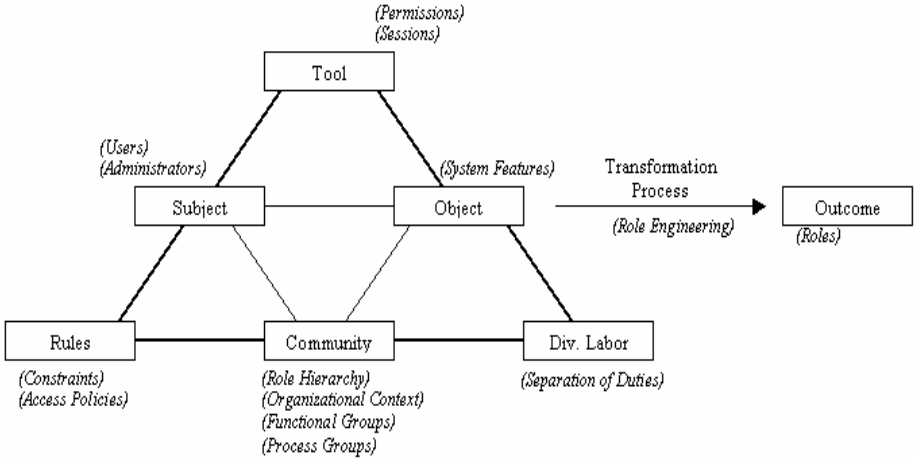

Figure 3. Adapted Engestrom's extended Activity System Model. (1997)

RBAC with Activity Theory

Figure 4 shows RBAC96 model with corresponding Engestrom's extended Activity System Model (1997) in grey parentheses. This shows individual applicability of specific Activity System Model Element with RBAC component. What this translates to is that in designing roles, for any specific RBAC component, more information and further analyzes could be carried out using specific activity theory principles as presented in grey next to them.

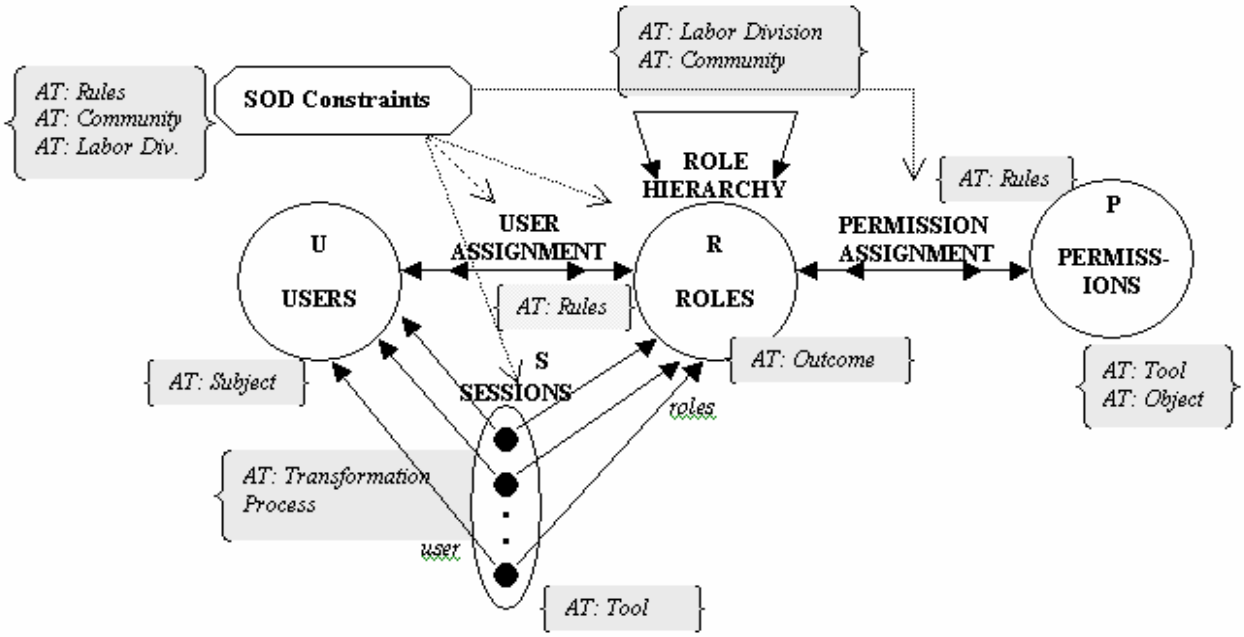

Figure 4. RBAC96 (Sandhu et. al, 1996) with Activity Theory's System Components

REAL-WORLD CASE STUDY: AN EXAMPLE

I carried out a case study at mid-sized US financial institution to further explore how role engineering is performed in organizations and how the activity theory principles and concepts can aid managers and designers engineer effective and secure roles. There were 6 people at the financial institution who aided us understand their role engineering process. I met them to 1) educate them on activity theory and theory behind RBAC though they were not aware of terms used for formal RBAC representations. Table-1 shows the appointments and meetings that were schedule with them. Due to space restrictions and ensuing work for further research on this and extended case study, I am only presenting partial details here to illustrate applicability and relevance of activity theory in role engineering.

Meeting #	Duration	Agenda
1	2 hours	*Explain the research objectives and gather general feedback and comments*
2	3 hours	*Present formal Activity Theory and RBAC systems*
3	2 hours	*Gather information on role engineering process carried out at the financial institution*
4	4 hours	*Run the case by them and solicit feedback on which principles and concepts of activity theory would they use most for specific components of the RBAC model*
5	2 hours	*Confirm and vet the documented process of their selections*

Table1. Schedule of Meetings and Agenda

The case

Based on discussions with the managers at the financial institution, we collectively came up with a situation where role engineering process can utilize activity theory principles to better understand the implications of role engineering process. Also, this will aid managers understand and unravel social and community-based facets of environment that are ignored in traditional role engineering process.

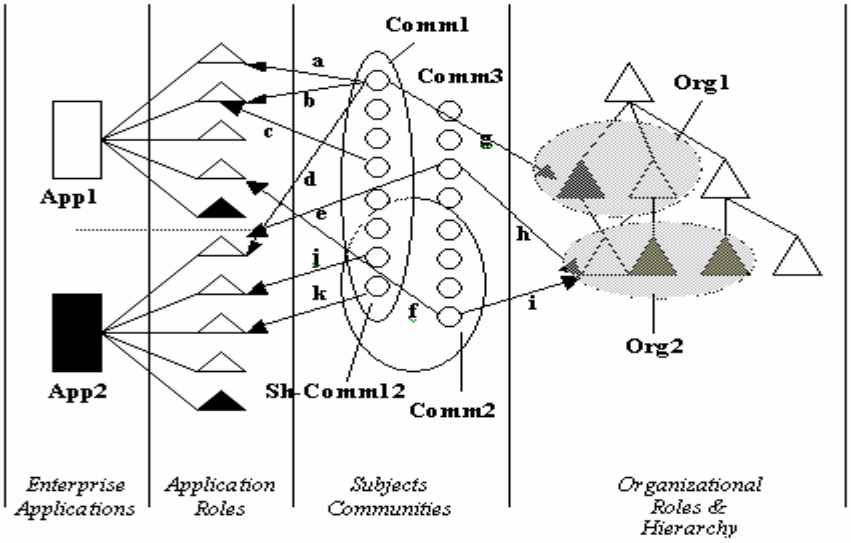

Figure 5. Role Engineering Components: real world case

Note on case: In the Figure 5, App1 and App2 are two applications for which the roles are to be engineered. The triangles in the section right of applications are application roles. In the subjects' section, circles are users and ovals represent

Assignments	Mappings	Emphasis
a	$User(Comm1)_1$-$Role(App1)_1$	User-role
b	$User(Comm1)_1$-$Role(App1)_2$	User-role
c	$User(Comm1)_2$-$Role(App1)_2$	User-role
d	$User(Comm1)_1$-$Role(App2)_1$	User-role
e	$User(Comm3)_1$-$Role(App2)_1$	User-role
f	$User(Comm2)_1$-$Role(App1_1$	User-role
g	$User(Comm1)_1$-Org_1	User-org
h	$User(Comm2)_1$-Org_2	User-org
i	$User(Comm2)_1$-Org_2	User-org
j	$User(Sh\text{-}Comm12)_1$-$Role(App2)_2$	User-Community
k	$User(Sh\text{-}Comm12)_1$-$Role(Appi2)_3$	User-Community

Table2. User assignments to roles

user communities (Comm1-3). Shared communities are the communities that are belonged by same users (Sh-Comm12). Only one such community is shown in the figure to keep the case simple. Right most section shows organizational roles within the enterprise (Org1 and Org2). These can denote same functional or positional roles in an organization.

The small cased letters in Figure 5 denote assignments of application roles and organizational roles to users. Table 2, below, show assignments with the exact mappings with the users, communities, roles and applications. Third column (Emphasis) presents the linkage that is most vital in understanding applicability of activity theory to role engineering for this scenario (Figure 5).

The basic principles of Activity Theory (Kaptelinin and Nardi, 1997)

The basic principles of Activity Theory include the hierarchical structure of activity, object-orientedness, internalization/externalization, tool mediation, and development. The following are some of the more important principles:

Hierarchical structure of activity (HSA)

The unit of analysis is an activity directed at an object that motivates activity, giving it a specific direction. Activities, actions and operations make up the three levels of activity.

Object-orientedness (OO)

The principle of "object-orientedness" states that human beings live in a reality that is objective in a broad sense: the things that constitute this reality have not only the properties that are considered objective according to natural sciences but socially/culturally defined properties as well.

Internalization/externalization (IE)

Activity Theory differentiates between internal and external activities. It emphasizes that internal activities cannot be understood if they are studied separately from external activities, because they transform into each other.

Mediation (MED)

Activity Theory emphasizes that human activity is mediated by tools. Tools are created and transformed during the development of the activity itself and carry with them a particular cultural-historical context.

Table 3 below represents different interactions amongst the user assignments (column 2) and how they result in various threats to specific component of RBAC (column 3). Column 4 in Table 3 represents Unit of focus or the component that is most likely be hit due to that particular interaction of assignments. The last column provides description of the interaction.

SCENARIO	INTERACTION	RESULT	UNIT OF FOCUS / THREAT	DESCRIPTION
I	a + b	Multiple role	User	*One user having more than 1 role in the same application*
II	b+ c	Shared role	Role	*Same application role assigned to multiple users from the same non-shared community*
III	a+ d	Cross-application roles	User	*One user assigned roles from multiple applications*
IV	a+ c	Community Role	Community	*Multiple users from the same community having access to multiple roles in same application*
V	d + e	Across-community role	Role	*Users from multiple communities having access to the same role*
VI	j + k	Shared Community application	Application	*Users from shared communities access multiple roles from same application*
VII	e + h & d + g	Across Org. role	Role	*Same application role assigned to users from multiple organizational role*
VIII	a +b + g	Across application role	Application	*Users from same organizational role have access to different application roles*
IX	f + I & e + h	Across application and org role	Applications	*Users from same organizational role have access to different roles from different applications*

Table 3. Interaction amongst assignments and resulting threat

Tables 4 and 5 are legend tables for further analyses done understand applicability of activity theory in role engineering as presented in Table 6.

Abbrev.	AT System Elements (Engestrom's System Model, 1997)
Tool	**To**
Subject	**S**
Object	**Ob**
Rules	**R**
Community	**C**
Division of Labor	**D**
Transformation Process	**Tr**
Outcome	**Ot**

Table 4. Legend for AT System Elements used in Table 6

Abbrev.	Role Engineering Components (refer Figure 4]
UA	User Assignment
PA	Permission Assignment
SOD	Separation of Duties Constraints
ARH	Application Role Hierarchy
ORH	Organizational Role Hierarchy
S	Sessions

Table 5. Legend for RBAC Components used in Table 6

Based on discussions with the managers at the financial institution where this case study was carried out and analyses of the case study dynamics, managers consented on applicability of different principles and concepts of Activity Theory, as they would apply to role engineering process. The threat scenario number from table 3 is presented in column 1 in table 6. Table 6, below, shows which component and consideration in the role engineering process (column 2) would be affected by Threat

Scenario (refer Table 3]	Role Engineering Components (Table 5, Figure 4)	Activity Theory Artifact (Kaptelinin and Nardi, 1997)	Activity Theory System Elements (Engestrom's System Model, 1997) (Table 5)
I	UA, PA, SOD	HSA, MED	S, To, D, Tr
II	SOD, ARH	OO, HSA	To, S, Ob, C, D
III	SOD, UA, ARH	HSA, MED	Ob, S, D, Tr
IV	UA, ARH, ORH	IE, OO	S, D, Tr, C
V	UA, ORH	IE, MED	S, Ob, T, C, D
VI	ARH, ORH, PA	IE, OO	S, Ob, T, C, D
VII	ORH, PA	HAS, IE	S, T, C, Tr, To
VIII	ARH, ORH, UA	IE, MED	S, T, C, Ot
IX	ARH, ORH, UA	IE, MED	S, Ob, T, C, D, Ot

Table 6. Application of Activity Theory to Role Engineering

Scenario (Table 3). Next columns in any row (read threat scenario) of the table present Activity theory principles (from both Kaptelinin and Nardi, 1997 model and Engestrom's System Model, 1997) that should be used to further unravel any interactions that may arise inefficient and insecure roles. For example, row 3 of the table represents Threat Scenario III (arising due to Cross-application roles). For this scenario user-assignment to roles, separation of duties and application role hierarchy are the most important components of RBAC that should be closely scrutinized. At the same time, managers at the financial institutions, feel that *Internalization/externalization (IE) and Object-orientedness (OO)* are the principles from Kaptelinin and Nardi (1997)'s Activity Theory Artifact that can aid in further understanding of the social dynamics within organization that can uncover some vital scenarios that should be accounted for in role engineering. Similarly, last column shows Activity Theory System Elements, consideration of which will significantly mitigate the risks of insecure role creation by analyzing the context of the users and roles (both application and organizational).

CONCLUSION

In the paper I discussed concepts and frameworks of roles, role-engineering and activity theory. Some common drawbacks of traditional role-engineering processes were presented. In light of unique insights that activity theory can provide in the role-engineering process to enable creation and maintenance of scalable and secure roles, I presented on how different components of RBAC model and of activity theory can be brought together for activity theory guided role-engineering. Then, I presented a case study of two applications from a northeast-US financial institution. With the help of 6 key people at the bank, we demonstrated how several threats (Table 6) that arise from social-and-community interactions and organizational-structure can be revealed using tenets of activity theory. Due to space limitations for AMCIS, I provided brief descriptions on the case study. More details on the underpinnings of the case study will be appearing in the updated version of this paper for a journal submission. As current and further research, I am in process of getting data from a couple of organizations to understand existing role structure and hierarchies and then use activity theory to understand how they can improved and also to examine any current threats. In wake of the emergence of roles in organizations and increased threats from insiders, it has brought to everyone's attention to find better ways to improve role-engineering processes. I believe, as is also demonstrated in the case study, that activity theory can be very effectively employed to design and engineer secure roles.

REFERENCES

1. Bertelsen and Bodker. (2003). Activty Theory, HCI Models, Theories, & Frameworks: Toward a Multidisciplinary Science. Carroll, J (ed)
2. Biddle B. and Thomas, E. (1979). Role Theory: Concepts and Research. New York: Robert E. Krieger Publishing Company, 1979.
3. Bodker, S. (1996). Applying activity theory to video analysis: how to make sense of video data in HCI. In B. A. Nardi (Ed.), *Context and consciousness: activity theory and human-computer interaction,* Cambridge and London, MIT Press, 69-103.Coyne. E. J. (1995). Role engineering. In *RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*, pages 4–5, New York, NY, USA, 1995. ACM Press.
4. Chaudhury, A., Mallick, D. and Rao, H.R. (2001). *Web channels in e-commerce***,** Communications of the ACM, Volume 44, Issue 1 (January 2001), Pages: 99 – 104
5. Coyne. E.J. (1996). Role engineering. In *Proc. of the ACM Workshop on Role-Based Access Control*, 1996.
6. Epstein P. and Sandhu. R. S. (2001). Engineering of role/permission assignments. In 17th Annual Computer Security Applications Conference, pages 127–136. IEEE Computer Society, Dec. 2001.
7. Engestrom, Y. (1987). Learning by expanding: An activity-theoretical approach to developmental research. Helsinki: Orienta-Konsultit Oy.
8. Engestrom, Y. (1999). Activity theory and individual and social transformation. In Y. Engestrom, R. Miettinen, & R.-L. Punamaki (Eds.), Perspectives on activity theory (pp. 19–38). New York: Cambridge University Press.
9. Engestrom, Y. and Miettinen, R. (1999). Introduction, in: Y. Engestr ¨om, R. Miettinen, R. Punam¨ aki (Eds.), Perspectives on Activity Theory, Cambridge University Press, Cambridge, 1999, pp. 1–16.
10. Epstein, P., Sandhu, R.S., (1999). Towards a UML based approach to role engineering. In: Proceedings of the 4th ACM Workshop on Role- Based Access Control, USA.
11. Epstein, P., Sandhu, R.S., (2001). Engineering of role/permission assignments. In: Proceedings of the 17th Annual Computer Security Applications Conference, USA.
12. Fernandez E. B. and Hawkins. J. C. (1997). Determining role rights from use cases. In *RBAC '97: Proceedings of the second ACM workshop on Role-based access control*, pages 121–125, New York, NY, USA, 1997. ACM Press.
13. Ferraiolo D. and Kuhn. R. (1992). Role-based access controls. In 15th NIST-NCSC National Computer Security Conference, pages 554–563, 1992.
14. Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. and Chandramouli. R. (2001). Proposed nist standard for role-based access control. *TISSEC*, 2001.
15. Floyd, C. (1987). Outline of a paradigm change in software engineering. In G. Bjerknes, P. Ehn, & M. Kyng (Eds.), Computers and democracy – A Scandinavian challenge (pp. 191-212). Aldershot, UK: Avebury.
16. Gallagher, M. P., O'Connor, A. and Kropp. B. (2002). The economic impact of role-based access control. *Planning report 02-1, National Institute of Standards and Technology*, March 2002.
17. He, Q., Antn, A.I., (2003). A framework for modeling privacy requirements in role engineering. In: Proceedings of the 9th International Workshop on Requirements Engineering (REFSQ'03), Austria.
18. Kaptelinin and Nardi B.A. (1997). Activity Theory: Basic Concepts and Applications, CHI tutorial, 1997
19. Kern. (2002). Advanced features for enterprise-wide role-based access control. In 18th Annual Computer Security Applications Conference (ACSAC 2002), pages 333–342. IEEE Computer Society, Dec. 2002.
20. Kern, M. Kuhlmann, A. Schaad, and J. Moffett. (2002). Observations on the role life-cycle in the context of enterprise security management. In *7th ACM Symposium on Access Control Models and Technologies*, June 2002.
21. Korpela, M., Soriyan, H. A. and Olufokunbi, K. C. (2000). "Activity Analysis as a Method for Information System Development." Scandinavian Journal of Information Systems(12): 191-210.
22. Korpela, M., Mursu, A. and Soriyan, H.A. (2002). Information systems development as an activity, Comput. Support. Coop. Work 11 (2002) 111–128.
23. Kuhlmann, M., Shohat, D. and Schimpf. G. (2003). Role mining - revealing business roles for security administration using data mining technology. In Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, pages 179–186. ACM Press, 2003.
24. Kuutti, K. (1991). Activity theory and its applications to information systems research and development, in: H.-E. Nissen, H.K. Klein, R. Hirschheim (Eds.), Information Systems Research: Contemporary Approaches and Emergent Traditions, Elsevier Science Publishers, Amsterdam, 1991, pp. 529–549.
25. Leont'ev, A. L. (1978). Activity, Consciousness, and Personality. Englewood Cliffs, NJ, Prentice Hall, 1978.
26. Mwanza, D. (2001). Where theory meets practice: A case for an Activity Theory based methodology to guide computer system design. INTERACT'2001, Oxford, UK, IOS Press.

27. Nardi, B.A. (1996). Activity theory and human-computer interaction. In B. A. Nardi (Ed.), *Context and consciousness: activity theory and human-computer interaction,* Cambridge and London, MIT Press, 69-103.
28. Neumann and M. Strembeck. G. (2002). A scenario-driven role engineering process for functional RBAC roles. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 33–42, New York, NY, USA, 2002. ACM Press.
29. RBAC Standard, Retrieved from http://csrc.nist.gov/groups/SNS/rbac/standards.html on 3/3/2008
30. Roeckle. H. (2000). Role-finding/role-engineering (panel session). In Proceedings of the 5th ACM workshop on Role-Based Access Control (RBAC 2000) [3], page 68.
31. Roeckle, H., Schimpf, G. and Weidinger. R. (2000). Process-oriented approach for role-finding to implement role-based security administration in a large industrial organization. In *RBAC '00: Proceedings of the fifth ACM workshop on Role-based access control*, pages 103–110, New York, NY, USA, 2000. ACM Press.
32. Rogers, Y. (2004) New theoretical approaches for HCI. ARIST: Annual Review of Information Science and Tech., 38.
33. Sandhu, R. S., Bhamidipati, V., Coyne, E. J., Canta, S. and Youman. C. E. (1997). The ARBAC97 model for role-based administration of roles: Preliminary description and outline. In Proceedings of the 2nd Workshop on Role-Based Access Control (RBAC 1997), pages 41–54, 1997.
34. Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman. C. E. (1996). Role-based access control models. IEEE Computer, 29(2):38–47, 1996.
35. Schaad, J. Moffett, and J. Jacob. (2001). The role-based access control system of a european bank: A case study and discussion. *In Proceedings of ACM Symposium on Access Control Models and Technologies*, pages 3–9, May-2001.
36. Stetsenko, A. (2005). Activity as object-related: Resolving the dichotomy of individual and collective planes of activity. Mind, Culture, and Activity, 12(1), 70–88.
37. Thomsen, D., O'Brien, D., Bogle, J., (1998). Role based access control framework for network enterprises. In: Proceedings of the 14th Annual Computer Security Application Conference.