V-Model Approach for Role Engineering

RADU CONSTANTINESCU, ANDREI TOMA, IULIANA SCORTA,
FLOAREA NASTASE, RAZVAN ZOTA
The Economic Informatics Department
Academy of Economic Studies
Bucharest, Piata Romana n° 62
ROMANIA
radu.constantinescu@ie.ase.ro, andrei.toma@ie.ase.ro, iuliana.scorta@ie.ase.ro,
nastasef@ase.ro, zota@ase.ro

Abstract: - Role engineering is a both necessary and critical topic in the development of Role Based Access Control system, which seems to be the most proficient approach nowadays. Despite the maturity of the RBAC model, the role engineering process is not a standardized approach. The paper aims to illustrate an enhanced process model for role engineering. The model is focused on the intuitive discovering of the roles and their assignment with permissions, and also the validation and verification of the results.

Key-Words: - access control systems, role based access control systems – RBAC, role engineering, authorization, roles, permissions, constraints, role hierarchies.

1 Introduction
The most sensitive characteristics of an information security system are linked to the approach of addressing the access control issue. For mature organizations, with clear defined responsibilities, the most suitable model is role based access control – RBAC [6], [7], [11]. The implementation of an access control model should be an important objective for the informational system implementation process. However, many organizations have already automated their business processes without taking in consideration access control as a mandatory and also extended approach. This is why a rigorous and comprehensive analysis has to be in order to achieve the correct permissions and role assignments as a prerequisite for implementing an access control system based on roles [1]. The efficiency of the whole engineering process depends on the ability of the designers to extract the correct assignments. For this purpose, a flexible methodology sustaining a coherent process of role engineering is required.

2 Problem Formulation
The objective of this paper is to design a process model for role engineering. The process model should be enforced by a specific methodology suited to identify the permissions and roles inside the information system of an organization and to identify also the assignments between those two sets. The methodology should support the design of role hierarchy and the identification of constraints.

Regarding the status of research in this area, features of role engineering have been discussed starting with Coyne’s paper. In this initial paper the main tasks of role engineering are defined. The mentioned tasks are: role definition, roles hierarchy definition, constraint definition and the mapping between roles and permissions [2].

Neumann and Strembeck have proposed an approach for role engineering based on scenarios [10]. In their model, each activity is described based on a set of scenarios and each scenario is then decomposed in several steps. Each step is then mapped to correspondent permissions. The approach has the disadvantage that it requires a great effort in order to comprehensively determine the possible scenarios.

Crook and Ince designed a conceptual framework for role engineering based on organizational structures. This approach helps determining roles but is not a comprehensive one [3]. Epstein suggested another approach of adding additional layers in order to ease role engineering. The approach is detailed in both top-down and bottom-up manner. The model takes the presumption that roles and permissions are already determined, so it doesn’t describe how those items will be defined. Neither the role hierarchy nor constraints definition is documented [5].

Goncalves and Maranda have proposed a role engineering method based on UML in correlation with system’s features. Functions are a middle layer between roles and permissions. A role can be mapped with several functions and each function will require access rights. The approach lacks non-functional items [8].
3 Problem Solution

3.1 Solution Overview

The paper presents an extended RBAC model, designed by the authors in order to enhance the role engineering process. The proposed model, VMRE-RBAC (V-Model Role Engineering RBAC), facilitates the decomposition of roles in permissions and then the results’ testing. The model is incremental and iterative. Every decomposition stage will have a correspondent testing stage and for every testing stage a new optimization of results is achieved. The testing stage is concerned with validation and verification of the results.

The paper is based on RBAC model. The components of the initial RBAC model are: users, roles, permissions and also the relations between those elements. The initial RBAC model has been enhanced by adding role hierarchies and constraints. RBAC96 cumulates those issues. One of the advantages of RBAC model is that it implements several major principles of computer security: least privilege, separation of duty and administration and also data-abstraction [9], [11]. The role engineering is a critical stage for any RBAC implementation. VMRE-RBAC model extends the standard RBAC model by adding extra layers between roles and permissions: profiles, tasks and steps. The roles are determined and defined starting from a well-known set of roles given the specific organizational structure. Those roles are associated with a set of goals and each goal determines responsibilities. Each responsibility is carried out through a specific profile. We suggest that profiles should be lower layer roles in the final role hierarchy. Each profile is then decomposed in tasks and the tasks are decomposed in steps. Steps are assigned to different sets of permissions. The decomposition can be driven by role or functionality issues.

After an initial decomposition process, the results will be tested incrementally. Testing means both verification and validation for the entities designed on each layer. In order to ease this process, we propose a set of nine properties which includes: equivalence, minimization, reuse, completeness, consistency and coherence. These properties are defined in order to obtain a simple, complete and non-equivocal model. The validation is driven by scenarios and responsibilities.

The model is flexible, new permissions, tasks, profiles and roles should be obtained in future iterations. Even new organizational responsibilities should be added to the existing roles by using profiles. The methodology contains all the steps needed for role engineering: identifying roles and permissions, mapping roles to permissions, identifying constraints and building role hierarchies.

As a start, we use the standardized RBAC96 relation between permissions and roles in order to build roles as a superset of permissions. We suggest decomposing the mapping of roles and permissions in several mappings between several middle layers. We propose the usage of three middle layers between roles and permissions, which are: profiles, tasks and steps. Each of these layers should be treated independently. The role engineering process consists in two main sub-processes. The first process is focused on a way to decompose the roles in permissions using a top-down approach. The second process tests the results using a bottom-up approach. The roles represent the upper layer of VMRE-RBAC model. A role is determined initially based on the work-profile of the company in which the model is applied. A role can be associated with several responsibilities. Each major responsibility is then associated with a specific profile. The proposed roles will be validated taking in account the goals of the activity which are elicited, defined and refined during the engineering process. Each user associated with a profile is responsible for a set of tasks specific to the organization. The validation of these tasks should be made by several test scenarios. The scenarios are designed as use-cases for the organization’s informational system. Each task can be interpreted as a set of multiple steps which are executed in a specific logical order. In the end, each step is related to a set of permissions. The grouping of multiple steps in a task determines the mapping between a set of permissions and a task. If a task is shared by different profiles, it will be reused. The same principle applies also to permissions, steps and profiles.

![Figure 1. Decomposition of roles in permissions](image-url)
In Figure 1, we present a schema of possible results of VMRE-RBAC decomposition process. For simplicity, the picture includes a single role $R_1$ which is linked to two profiles $Pf_1$ and $Pf_2$. For each profile we identified the tasks assigned. In this particular case, the profiles have multiple tasks assigned from which $Sc_2$ is shared. Also, there are several steps reused and each step implies at least one assigned permission.

### 3.2 VMRE-RBAC Model

The standard elements of RBAC model - users, roles and permissions - are also used in the proposed extension. RBAC standard defines the mapping between roles and permissions, as depicted in Figure 2, but it doesn’t explicit how this mapping is achieved. We aim to propose a role-engineering solution in this concern.

![Roles and permissions association in NIST’s RBAC standard](image)

We will detail the relation between roles and permissions starting from the NIST’s standardized RBAC model conventions:

- $R$ – roles set
- $P$ – permissions set
- $PA \subseteq P \times R$ association between permissions and roles

The general model for VMRE-RBAC is presented in Figure 3.

![Decomposition and testing in VMRE-RBAC](image)

Starting from the classic RBAC96 model, we added three middle-layers which are: profiles, tasks and steps. Each decomposition stage has an equivalent testing stage. In order to formalize the model, we use the following notations:

- $R$ – roles set
- $Pf$ – profiles set
- $Sc$ – tasks set
- $Ps$ – steps set
- $P$ – permissions set
- $RPf \subseteq R \times Pf$ – many to many relation between roles and profiles
- $PfSc \subseteq Pf \times Sc$ – many to many relation between profiles and tasks
- $ScPs \subseteq Sc \times Ps$ – many to many relation between tasks and steps
- $PsP \subseteq Ps \times P$ – many to many relation between steps and permissions

An important goal of the paper is to support a methodology which should optimize the process of mapping between roles and permissions. We suggest a series of operations that will help the role-engineering process: minimize the sets at every layer, reuse elements, verify if constraints are in place and verify the complete mapping between elements in adjacent sets. The testing and optimization criteria are formalized in nine properties. The properties deal both with the elements on the same layer and with the mappings between elements in adjacent layers. In other words, the properties apply both on elements and relations. The properties we propose are: equivalence, uniqueness, completeness, reused element, minimum, consistency and coherence. Properties like equivalence, uniqueness, completeness or reused element are also discussed in former papers as [5].

As we already mentioned, it is desirable that the number of roles, profiles, tasks and steps used in relations to be minimal. Ideally, each element is unique, the designer eliminates any duplicate. Additionally, the uniqueness of each element means that there is no other element that is equivalent to it. The equivalence can be demonstrated by comparing how sets of elements from a layer are mapped to elements on the upper layer. If there are equivalent elements, they should be minimized.

The role engineer verifies that all the roles defined have at least a permission assigned to it. Also, each element on one layer should be mapped to at least one element on both adjacent layers. This is formalized in the completeness property. The role engineer also test the consistency of each role and profile, meaning that the final set of permissions determined will sustain the achievement of all declared goals. The consistency of tasks is tested through scenarios.

The identification of constraints is one of the most challenging tasks in the design. It is important that all the constraints should be identified and tested. We propose the coherence property in this matter.

### 3.3 VMRE-RBAC Process

As we already stated, RBAC model has as a primary feature the many to many relation between roles and permissions. In VMRE-RBAC model, the RBAC model is...
The results of the role engineering process are:

- The decomposition process contains the following steps: identify the initial roles and role
  constrains, identify the major responsibilities and classify the candidate profiles and profile constrains,
  for each profile elicit the tasks and then define the steps, identify permissions and subsidiary constrains. The
  process is depicted in Figure 4.

![Figure 4. VMRE-RBAC process](image)

The testing process involves the verification and validation for all the elements and relations defined in
the decomposition stage. Verification means the process of evaluation applied to elements and relations in which
the results are confronted with the requirements and conditions defined by the designer. In the verification
stage will be used several properties that were already mentioned in the paper. On the other hand, validation
assures that the process is defining the right system. This implies that the designers should confront the results
with the beneficiaries. Also, validation implies that the designers should confront the results with the
beneficiaries in order to validate the profiles and roles. Scenario catalog: list of scenarios elicited with the
beneficiaries in order to validate tasks.

- RBAC model: role hierarchy, permissions’ set and the constraints applied.

## 4 Conclusions

The idea of this research is driven by the complexity of the existing role-engineering processes and the lack of a
standardized way for performing role engineering. The paper presents an approach for role engineering that
aims to simplify the engineering process by linking it directly to the logic of business. The model includes
both a decomposition process, from roles to permissions, and also introduces extra-layers in the RBAC standard
model. As a possible application, the model should be a prerequisite for an information security access control
system as the one presented in [4].

Even if the idea of adding new layers between the roles and permissions has been already discussed in a couple
of scientific researches, the VMRE-RBAC process model brings a new perspective for role engineering.
The VMRE-RBAC engineering process is also focused on the verification and validation of the results, an issue
that should improve the quality of the whole role based access control future implementation.

### References:

  University, 2002