Acta Technica *61*, No. 4B/2016, 197–206 © 2017 Institute of Thermomechanics CAS, v.v.i.

# Access control model based on role and attribute and formal verification[1]

Hui Qi[2], Hongxin Ma[3], Xiaoqiang Di[2], Jinqing Li[2]

**Abstract.** The defects of the current access control models based on role and attribute (RABAC) and their causes are analyzed and more fine-grained, flexible and efficient RABAC model are proposed. The evaluation indicators of access control model are extended to describe the access control granularity, flexibility and decision performance of model. The model described in this paper and other models are evaluated theoretically in these three aspects.

**Key words.** RBAC, ABAC, Attribute-based access control, access control, RABAC.

## 1. Introduction

Since the late 1960s when the access control matrix was proposed, access control technology has received much attention and gained considerable development. At present, lots of access control models have been proposed and applied. Among these access control models, Role-Based Access Control (RBAC) model has made great success [1]. By introducing a mid-layer (role) between users and permissions, the RBAC model can maintain the flexibility and security of the access control system facing large number of users, large amount of data and large scale of business. With the further development of information technology, the emergence of new computing models (such as ubiquitous computing, mobile computing and cloud computing) and the expansion of network environment (from Internet to mobile Internet, Internet of things, space-ground integration network) make access control requirements become more complex. Access control decisions depend more on the context in which the

[1] This work is supported in part by the National High Technology Research and Development Program (863 Program) of China under Grant No.2015AA015701, the Science and Technology Planning Project of Jilin Province under Grant No. 20150204081GX and Grant No. 20140312038ZX, the 13th Five-Year Science and Technology Research Project of the Education Department of Jilin Province under Grant No. 2016-378 and the Industrial Technology Research and Development Project of Jilin Province Development and Reform Commission under Grant No. 2014Y113.

[2] School of Computer Science and Technology, Changchun University of Science and Technology, Changchun, 130022, China

[3] Training Department, Aviation University of Air Force, 130022, Changchun, China

access control requests reside and the security attributes of subjects and objects. ABAC model was born in this environment, which solves the problem that the RBAC model cannot well support a large number of context attributes (the problem of role explosion) and achieves the dynamic and fine-grained access control [2]. However, the access control decision of ABAC model is more complex, hence the safety analysis of access control rules is more difficult.

Both RBAC and ABAC have their particular advantages and disadvantages, and their advantages are complementary. Therefore, some scholars put forward the RBAC/ABAC hybrid approach (namely RABAC model) to hold the simplicity and security of RBAC, as well as the flexibility of ABAC. RABAC model is based on RBAC, using RBAC to manage static relationship between users and permissions to ensure the security of this relationship, while using ABAC to manage dynamic relationship between users and permissions, that is, dynamically applying attribute-based access control rules to user-role mappings, role-permission mappings and user-permission mappings. Nevertheless, there are some deficiencies in current RABAC models with respect to access control granularity, flexibility and decision performance. This paper deeply studies these problems, proposes the improved RABAC model and verifies the new model theoretically.

The rest of this paper is organized as follows. Section 2 gives a brief introduction to the research of access control model. Section 3 presents the framework of the proposed access control model. In Section 4 three important properties of the model are verified in theory. Section 5 concludes this paper.

## 2. Related work

RBAC model maps the users to the roles, and then maps the roles to the permissions. It makes the management of access control be divided into two parts: the user-role mapping and the role-permission mapping, which simplifies the management of access control. After the RBAC96 model, in order to further improve the security of access control management, several models such as ARBAC97 model (Administrative RBAC97), ARBAC99 model and ARBAC02 model appeared successively [1]. The emergence of these models makes RBAC model more mature, greatly improving the security and the ease of use.

But RBAC model is not suitable for the environment where it is necessary to dynamically and finely control the user-permission mapping [3, 4]. In this environment, the relationship between users and roles and that between roles and permissions frequently changes. More roles are needed to support different access control requirements, which makes the RBAC model more complex and difficult to manage. Therefore, people put forward the ABAC model, using access control rules based on attribute to directly determine the relationship between users and permissions to achieve the dynamic and flexible access control. But ABAC also has disadvantages. Unlike RBAC, it does not have a set of strict rules to ensure the security of user-permission mapping. In the face of a large number of access control rules, the security analysis becomes very difficult. For the problems existing in ABAC and RBAC, many scholars have put forward the new access control model (RABAC) that combines ABAC and RBAC. Literature [5] proposed 3 ways to introduce ABAC into RBAC: Dynamic Roles, Attribute Centric and Role Centric, the third of which is the better RBAC/ABAC hybrid approach and is widely accepted, but Literature [5] does not make a detailed description of the scheme.

Literature [6] proposed a fine-grained access control model based on role and attribute for web applications and designed the method for verifying the model and that for automatically generating code. The model is based on RBAC and uses attribute-based policies to finely control permissions. Literature [7] proposed role-centric attribute-based access control model of which the access control decision-making process is divided into two stages: first use RBAC to determine all the permissions available to the user in the current session, and then use permission filtering policy (PFP) to extract the final available permissions. The PFP constrains the available set of permissions based on environment, subject and object attributes. The retrieval of PFP depends on the object attributes. Literature [8, 9] proposed a more flexible retrieval approach than Literature [7]. The retrieval approach not only supports object identifiers, but also supports query expressions based on object attributes. Literature [10] proposed a framework integrating attribute-based policies into RBAC. Different from the literature [7, 8], this framework does not apply the attribute-based policies after the establishment of all the permissions available to the user, but it applies the policies during the process of establishing available permissions, e.g. using attribute-based policies to filter user-role relationships and role-permission relationships independently just after the establishment of these relationships.

Literature [11] proposed a generic framework for access control model, under which it researched the two important properties: monotonicity and completeness and then it applied the two properties to evaluate and design different ABAC models. Literature [12], [13] studied the expressive power of access control model qualitatively and quantitatively, which is similar to the completeness of the literature [11]. This paper defines new properties for RABAC model on the basis of the literature [11]: access control granularity, flexibility and decision performance.

## 3. Model overview

The proposed access control model in this paper is based on the RBAC / ABAC hybrid approaches proposed in the above literatures, and solves some problems in these approaches. This section will show a framework for the new model which makes some improvements to the framework in the literature [10] and describes the composition of the framework and the access control workflow.

### *3.1. The composition of framework*

The framework of the access control model is shown in Fig. 1. The model is divided into upper and lower parts. The upper part uses the RBAC model to control the static part of access control that is the static relationship between users and permissions, while the lower part uses the ABAC model to control the dynamic part of access control that is reducing the number of permissions associated with a user by attribute-based access control rules.

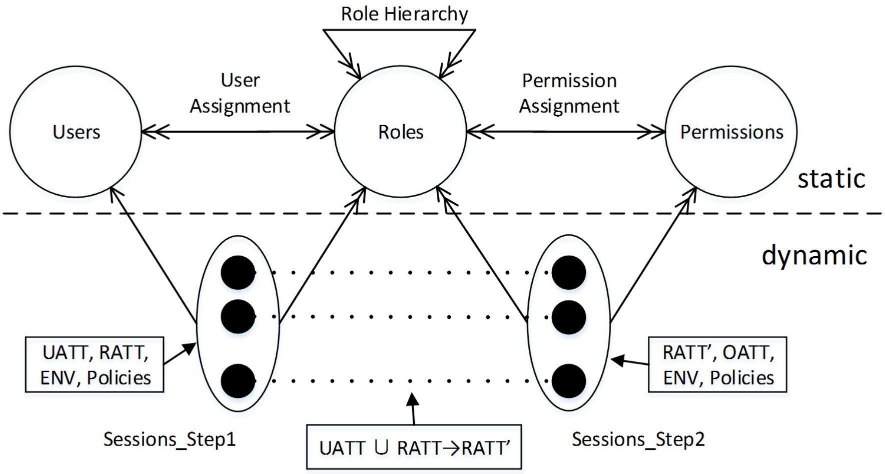

Fig. 1. Framework of the access control model

In the static part of the model, we retain most of the elements of the RBAC model, including users, roles, permissions (Permissions can be subdivided into operations (OPS) and objects (OBS), where Permissions $\subseteq$ OPS$\times$OBS). We regard objects as the attributes of operations so that Permissions=OPS), user-role relationships (UA), role-permission relationships (PA) and role inheritance relationships (RH). In addition, we also define the user attributes (UATT) for users, define the roles attributes (RATT) for roles and define the object attributes (OATT) for permissions. These attributes will be involved in the dynamic part of the model to filter permissions, namely to reduce the permissions of a user.

In comparison with the access control model proposed in the literature [10], the model of this paper is more fine-grained. The literature [10] also applies the attribute-based access control policies to the user-role relationships and the role-permission relationships respectively, but when applying the policies to role-permission relationships, it uses the simple role attributes (RATT), while this paper uses the new RATT' combined with UATT, that is introducing UATT into RATT to form the new RATT' during the transition from Sessions_Step1 to Sessions_Step2. Because RATT' contains the user attributes, the model of this paper can finely control the role-permission relationships. For example, using the model of this paper, we can define that the role of an organization (Organization is usually a user attribute.) is not able to activate a certain permission, which is not supported by the model of the literature [10].

In this paper, UATT is introduced into RATT, for in the RBAC model, the role can be seen as the agent of the user that represents the user to establish the association with the permission. So it is reasonable to add user attributes to role attributes before performing Sessions_Step2.

### 3.2. Access control workflow

The above gives the overall structure of the model including the static composition and the dynamic composition, which is the static description of the model. This section will describe how the components of the model are involved in the process of access control decision, namely the dynamic description of the model. In this paper, the process is called the access control workflow, which is defined as follows:

1. Use the RBAC model to determine the user-role mappings, that is U→R.
2. Remove the mappings that violate the access control rules from U→R according to UATT, RATT, ENV and the corresponding policies so that the new user-role mappings (U→R', U→R'⊆U→R) are built.
3. Use the RBAC model to determine the role-permission mappings (R'→P), and combine UATT and RATT to build the new role attributes (RATT', RATT'=UATT∪RATT).
4. Remove the mappings that violate the rules from R'→P according to RATT', OATT, ENV and the corresponding policies so that the new role-permission mappings (R'→P', R'→P'⊆R'→P) are built.

After performing the above steps, we get the final user-permission mappings U→P', which is the subset of user-permission mappings determined by the RBAC model, that is U→P'⊆U→P. Since the security of U→P is guaranteed by the RBAC model and the access control model of this paper only removes some invalid mappings from U→P, the final user-permission mappings U→P' does not violate the constraints of the RBAC model. This is the strategy adopted by the current RABAC model. ABAC is used to filter the user-permission mappings U→P determined by RBAC. Therefor the security of the model is guaranteed and the dynamic and fine-grained access control can be achieved as well.

The access control workflow is actually the process of session establishment. The model of this paper extends the session in the RBAC model. In RBAC, the session only establishes the user-role mappings, while the session of this paper has to establish the role-permission mappings in addition to establishing the user-role mappings. When the establishment of session is completed, the process of access control decision will be over. Thus, it is unnecessary to apply the attribute-based policies after the session is established, which is different from the access control decision in the literature [7, 8]. The section 4 will compare the two decision-making methods.

## 4. Model verification

Verification of access control model, in particular, formal verification has been a difficult problem. Literature [7, 8, 10] has not verified the model, but these literature have pointed out that the formal analysis and verification of the model is very important, and it is the direction of future efforts. Literature [11] defines two properties for access control model: completeness and monotonicity. Since these two properties refer to the calculation rules of access control decision and our model does not take into account the specific decision-making process, the two properties are not discussed in this paper.

This paper extends the properties of the literature [11], defines new properties suitable for RABAC model: access control granularity, flexibility and decision performance, and theoretically proves that the model in this paper is superior to the model in the literature [7, 8, 10] in these three aspects.

### *4.1. Access control granularity*

Whether it is RBAC, or ABAC or hybrid model, the goal of the model is to determine the relationship between users and permissions, that is, the permissions a user can obtain in the current session. In order to achieve this goal, the RBAC model statically connects users with permissions through roles; ABAC uses attribute-based access control rules to dynamically determine the user-permission relationships; The hybrid model first uses RBAC to determine the static relationships between users and permissions, and then uses ABAC to dynamically reduce the user-permission relationships. Both the model in this paper and the model in the literature [7, 8, 10] use the approach of hybrid model, that is, first determine the static relationships, and then use attributes to dynamically reduce the relationships. The difference of these models is the way of reducing the user-permission relationships. In the process of reducing the relationships they require various attributes. Therefore, this paper uses the usage of attributes as the measure of access control granularity of the model.

The access control granularity of a RABAC model depends on the maximum number of attributes available in the process of reducing the user-permission relationships.

Based on the above measurement, we can compare the access control granularity of different RABAC models. First, we have to determine which attributes are used when reducing the user-permission relationships. Formal analysis shows that the model in the literature [7, 8] first uses RBAC to generate the ordered pairs consisting of user and permission (UP, UP⊆USERS×PERMS, and then uses attribute-based policies to determine whether each pair <u, p> in UP is active or not, which in fact establishes the mapping of UP onto the set {T, F}. When building the mapping, the model needs to use the user attributes and the permission attributes. The mapping can be expressed as

$$\mathrm{up\_tf} : \mathrm{UP} \times 2^{\mathrm{UATT}} \times 2^{\mathrm{OATT}} \times 2^{\mathrm{ENV}} \to \{\mathrm{T}, \mathrm{F}\}\,. \tag{1}$$

In the mapping up_tf, dom(up_tf) includes $2^{\mathrm{UATT}} \times 2^{\mathrm{OATT}} \times 2^{\mathrm{ENV}}$, where UATT is the user attributes, OATT denotes the object attributes which can be seen as the permission attributes and ENV stands the environment attributes.

From the structure of dom(up_tf), it is concluded that the maximum number of attributes available in determining the relationship between UP and $\{T, F\}$ is: $|\mathrm{UATT}| + |\mathrm{OATT}| + |\mathrm{ENV}|$. The key of the above analysis process is to make clear the mapping structure of UP onto $\{T, F\}$, and then to calculate the access control granularity of the model according to the application of the attributes.

Applying this analysis method to the model in the literature [10], we can calculate the access control granularity of this model. The feature of the model is that the access control decision-making process is divided into two stages. The first stage uses RBAC to build the set of ordered pairs consisting of users and roles (UR, UR⊆USERS×ROLES), and then build the mapping of UR onto T, F. Because the role is the set of permissions, the mapping cannot determine whether each pair <u, p> is active or not. So the first stage does not imply the access control granularity of the model. In the second stage, the model first uses RBAC to establish the set of ordered pairs composed of roles and permissions (RP, RP⊆ROLES×PERMS). Because the role can be regarded as a user agent, the establishment of the set RP implies that the set UP is set up, and the subsequent attribute-based policies also act on the set UP. According to the description of the literature [10], the second stage of the establishment of the mapping of UP onto T, F can be expressed as

$$\mathrm{up\_tf} : \mathrm{UP} \times 2^{\mathrm{RATT}} \times 2^{\mathrm{OATT}} \times 2^{\mathrm{ENV}} \rightarrow \{\mathrm{T}, \mathrm{F}\}\,. \tag{2}$$

From the structure of equation (2), it is known that the access control granularity of the model is |RATT|+|OATT|+|ENV|. In the equation (1), UATT contains RATT, namely RATT⊆UATT, we have |RATT|<|UATT|. Therefore, the model in the literature [7, 8] is more fine-grained than the literature [10].

The model of this paper is also divided into two stages, the first stage is the same as the literature [10]. The difference is the second stage. This paper modifies the structure of equation (2), which is changed to

$$\mathrm{up\_tf} : \mathrm{UP} \times 2^{\mathrm{RATT}'} \times 2^{\mathrm{OATT}} \times 2^{\mathrm{ENV}} \rightarrow \{\mathrm{T}, \mathrm{F}\}\,. \tag{3}$$

In equation (3), RATT'=UATT∪RATT. So, equation (3) is equivalent to

$$\mathrm{up\_tf} : \mathrm{UP} \times 2^{\mathrm{UATT}} \times 2^{\mathrm{OATT}} \times 2^{\mathrm{RATT}} \times 2^{\mathrm{ENV}} \rightarrow \{\mathrm{T}, \mathrm{F}\}\,. \tag{4}$$

The structure of equation (4) shows that the access control granularity of the model in this paper is the same as the literature [7, 8], but it is better than that in literature [10].

### 4.2. Flexibility

We can find that the model of this paper not only has the mapping like equation (1), but also has the mapping of UR onto {T,F}

$$\mathrm{ur\_tf} : \mathrm{UR} \times 2^{\mathrm{UATT}} \times 2^{\mathrm{RATT}} \times 2^{\mathrm{ENV}} \rightarrow \{\mathrm{T}, \mathrm{F}\}\,. \tag{5}$$

Without consideration of the impact of the attributes and the environment, the model of this paper contains two mappings: UR→{T,F}and UP→{T,F}. These two mappings can be rewritten as: U×R→T,F and U×P→{T,F}, where U represents USERS, R represents ROLES and P represents PERMS. Since R is a collection of

P, these two mappings can be integrated into the mapping

$$\mathrm{upp\_tf} : \mathrm{U} \times 2^{\mathrm{P}} \rightarrow \{\mathrm{T}, \mathrm{F}\} . \tag{6}$$

The mapping of UP onto {T, F} in the literature [7, 8] can be written in this general form like the equation (6) without considering the attributes and the environment. So we can give the measure of flexibility.

The measure of flexibility is the maximum capacity of the set dom(upp_tf), namely the value of $|dom(upp\_tf)|$.

According to the above measure, we can easily draw that the model of this paper is more flexible than the model in references [7, 8] because of $|\mathrm{U}{\times}2^{\mathrm{P}}|{>}|\mathrm{U}{\times}\mathrm{P}|$. The model proposed in this paper has the same flexibility as the model described in [10] because both of them have the same structure of dom(upp_tf), which is $|\mathrm{U} \times 2^{\mathrm{P}}|$.

### *4.3. Decision performance*

In this paper, the decision performance of the model reflects the execution speed of the model. For the RABAC model, the decision performance is mainly determined by the speed of executing the access control policies. For in the access control decision-making process, the process of using RBAC to determine the user-role relationships and the role-permission relationships is the same to each RABAC model. The difference among these models is the attribute-based policies. The policies in this paper and the policies in the literature [10] refer to the mapping of the equation (1) and the mapping of the equation (5). The policies of the literature [7, 8] only refer to the mapping of the equation (1). Without considering the attributes and the environment, the size of the policy set of the two models is different, so the performance of the policy retrieval is also different. As a result, the size of the policy set is the measure of performance.

For the model of this paper and the model of the literature [10], the policy set can be simplified as: U×R→{T,F} and U×P→{T,F}. Since the latter is determined by the role-permission relationships, it can be rewritten as R×P→{T,F}. In this way, the maximum size of the policy set of the model is

$$|\mathrm{U} \times \mathrm{R}| + |\mathrm{R} \times \mathrm{P}| = |\mathrm{U}| \times |\mathrm{R}| + |\mathrm{R}| \times |\mathrm{P}| = |\mathrm{R}|(|\mathrm{U}| + |\mathrm{P}|) . \tag{7}$$

For the model in literature [10], the policy set can be simplified as U×P→T,F. The maximum size of the policy set of the model is

$$|\mathrm{U} \times \mathrm{P}| = |\mathrm{U}| \times |\mathrm{P}| . \tag{8}$$

Comparing with equation (8), the value of equation (7) is smaller because the number of roles is usually smaller than the number of users and the number of permissions. Assuming that the number of users is the maximum value, and the number of roles is the minimum value, in the equation (7), the value $|\mathrm{R}|{\times}|\mathrm{U}|$ plays a decisive role, which must be smaller than the value $|\mathrm{U}|{\times}|\mathrm{P}|$. Theoretically speaking, the model of this paper is superior to the model of the literature [7, 8] in decision performance.

## 5. Conclusion

In this paper, we deeply analyse the problems existing in the RABAC model and propose an improved model. We also study the formal verification of the RABAC model, analyzing the access control granularity, flexibility and decision performance of the model, proposing the formal method for analyzing these 3 characteristics, and using this method to compare the differences between the new model and other RABAC models. We theoretically prove that the new model is superior to other RABAC models in these 3 characteristics. The formal verification method in this paper provides the evaluation method and the improvement direction for the RABAC model. In future research, we will carry out quantitative analysis of other properties of the RABAC model, will continue to improve the access control model using the quantitative measures, and will try to extend this formal verification method to other access control models.

### References

[1] E. Sahafizadeh, S. Parsa: *Survey on access control models.* Proc. IEEE 2nd IC Future Computer and Communication (ICFCC), 21–24 May 2010, Wuhan, China, paper V1 1–3.

[2] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miler, K. Scarfone: *Guide to attribute based access control (ABAC) definition and considerations.* NIST Special Publication 800–162. 2014

[3] L. Cirio, I. F. Cruz, R. Tamassia: *A role and attribute based access control system using semantic web technologies.* Proc. OTM Confederated IC On the move to meaningful internet systems, Vilamoura, Portugal, 25–30 Nov. 2007, Volume Part II, 1256–1266.

[4] V. Suhendra: *A survey on access control deployment.* Series "Communications in Computer and Information Science (CCIS)" *259*, 11–20.

[5] D. R. Kuhn, E. J. Coyne, T. R. Weil: *Adding attributes to role-based access control.* Computer *43* (2010), No. 6, 79–81.

[6] S. H. Ghotbi, B. Fischer: *Fine-grained role- and attribute-based access control for web applications.* Commun. Comp. Info. Sci. (CCIS) *411* (2013), 171–187.

[7] X. Jin, R. Sandhu, R. Krishnan: *RABAC: Role-centric attribute-based access control.* Proc. 6th IC on Mathematical Methods, Models and Architectures for Computer Network Security, 17–19 Oct. 2012, St. Petersburg, Russia, 84–96.

[8] Q. M. Rajpoot, C. D. Jensen, R. Krishnan: *Attributes enhanced role-based access control model.* Lecture Notes in Computer Science *9264*, Springer Verlag, 3—17.

[9] Q. M. Rajpoot, C. D. Jensen, R. Krishnan: *Integrating attributes into role-based access control.* Lecture Notes in Computer Science *9149*, Springer Verlag, 242—249.

[10] J. Huang, D. M. Nicol, R. Bobba, J. H. Huh: *A framework integrating attribute-based policies into role-based access control.* Proc. 17th Symposium on Access Control Models and Technologies, 20–22 June 2012, Newark, New Jersey, USA, 187–196.

[11] J. Crampton, C. Morisset: *Monotonicity and completeness in attribute-based access control.* Proc. 10th International Workshop Security and Trust Management, 10–11, Sept. 2014, Wroclaw, Poland, 33–48.

[12] W. C. Garrison III, A. J. Lee, T. L. Hinrichs: *An actor-based, application-aware access control evaluation framework.* Proc. 19th ACM Symposium on Access Control Models and Technologies, 25–27 June 2014, Ontario, Canada, 199–210.

[13] W. C. Garrison III, A. J. Lee: *Decomposing, comparing, and synthesizing access control expressiveness simulations.* Proc. IEEE 28th IEEE Computer Security Foundations Symposium and Affliated Workshops, 13–17 July, Verona, Italy, 2015, CD-ROM.

Received November 16, 2016