Debit: A Diversity-based Method for Implicit Role Transition in RBAC Deployments

Shanshan LI, Qingbo WU, Lianyue HE, Lisong SHAO, Jie YU
School of Computer
National University of Defense Technology
Changsha, China
{shanshanli, qingbo.qu, lianyuehe, lisongshao, jieyu} @nudt.edu.cn

***Abstract*-Role-based access control (RBAC) is a widely used access control paradigm in operating system due to its simplicity, scalability and fine-grained control ability. Current approaches need re-login to transit role when the permissions of assigned role are inadequate for operation. This usage is easy for secure administration, while inflexible in practical use, especially for those authenticated users. This paper describes a diversity-based access control model supporting implicit role transition, called DRT-RBAC. By measuring users' authentication trustworthiness, a range for role transition can be computed, and user whose diversity between the old role and the new one fall into this range is allowed for automated role transition. Further, we propose Debit, which calculates the diversity between roles in operating system through an analytic hierarchy process. In Debit, the roles are decomposed to fine grained system privileges, capability. Debit computes a weight for each category of capability through constructing a pair wise comparisons matrix. The diversity of two roles is finally obtained based on the weight of each capability category and the number difference of capabilities on the category. We implement Debit in Centos 5.4 to support implicit role transition based on Authentication Trustworthiness of login user.**

Keyword-DRT-RBAC; authentication trustworthiness; Debit.

I. INTRODUCTION

Access control is an indispensable component of operating system, which mediates requests to resources of the system and makes decisions about whether or not they should be granted. Relative to Classical Discretionary Access control (DAC), Mandatory Access Control (MAC), Role-based Access Control (RBAC) model is more emphasized recently due to its simpleness, scalability, fine-grained control ability, and has been proven to be efficient to improve security administration with flexible authorization management. In RBAC, users are assigned to roles, and permissions are granted to roles. The protection state is characterized by the triple <UA, PA, RR>, where UA is the user-role assignment relation, PA is the permission role assignment relation and RH is a role composition in systems. RBAC can greatly simplify the management of authorizations within a system, because a group of subjects are usually given the same permissions.

For many mainstream operating systems, a user is generally assigned a role either selected in system authentication module or based on the least privilege principle. For ease of secure administration, once the permissions of assigned role are inadequate for operation, the user need re-login and select another role from his available list. Actually, if user can pass strong authentication, he is well trustworthy and should be allowed to transit role transparently. Current usage of roles requires manual intervene of users, thus inflexible in practical use.

In this paper, we investigate a diversity-based access control model supporting implicit role transition, called DRT-RBAC. DRT-RBAC model associates the strength of authentication trustworthiness with a transition range of role, which takes the diversity between roles as the decision condition to transit role. Only those users whose diversity between the old role and the new one fall into the transition range can make transition implicitly. The model keeps the advantage of permission management, while emphasizes on the flexibility of user-role assignment and makes operating system friendly to users.

Based on DRT-RBAC model, we propose Debit, an analytic hierarchy process to measure the diversity between roles in operating system. Debit analyzes the inherent factors which result in the difference among roles, and constructs a hierarchy with fine-grained system privileges, capability, each layer is analyzed independently. Through constructing a pair wise comparisons matrix, Debit computes a weight for each category of capability. The diversity of two roles is finally obtained based on the weight of each capability category and the number difference of capabilities on the category.

The rest of this paper is organized as follows. We briefly review the related work in Section 2. In Section 3, we present some basic knowledge, including the concept of authentication trustworthiness in single and multiple authentication mechanisms. In Section 4, we describe the diversity-based RBAC model DRT-RBAC supporting implicit role transition, and present an analytic hierarchy process Debit to calculate diversity. In Section 5, we implement Debit in Centos 5.4 and verify its effectiveness. We conclude the work in Section 6.

II. RELATED WORK

One of the most challenging problems in managing operating systems is the complexity of security administration. Role-based access control has become the predominant model for advanced access control since it reduces the cost of security management. There has been

 ISBN: 978-1-61208-153-3

much work done to explore the role assignment, time constraint and security controlled mobility to enhance the network performance.

Odell and Parunak [1] found that an important characteristic of real-world systems is that the roles of subject may change over time. These changes can be of several different kinds. They analyze and classify the various kinds of role changes over time that may occur, and show how this analysis is useful in developing a more formal description of the application. Liao and Hong [2] found that IRBAC 2000 model [3] had not considered the separation of duties, and they analyze the scenarios where dynamic role translations violate statically mutually exclusive role constraints, then propose a protective mechanism utilizing prerequisite conditions to enforce the security of the IRBAC 2000 model. These works provide guide for role transition among multiple domains in theory; however, they are not fit for local role transition, especially for operating system.

Some works consider role transition from temporal and spatial perspective [4-7], that is, roles of subject may change in different time periods and environments. Bertino et al. proposed the Temporal-RBAC (TRBAC) model that addresses some of the temporal issues related to RBAC [8]. The main features of this model include periodic enabling of roles and temporal dependencies among roles which can be expressed through triggers. James, et al. argued that TRBAC model addresses the role enabling constraints only. They proposed a Generalized Temporal Role-based Access Control (GTRBAC) model capable of expressing a wider range of temporal constraints [9]. In particular, the model allows expressing periodic as well as duration constraints on roles, user-role assignments, and role-permission assignments. Joshi and Ghafoor [10] showed how RBAC can be extended to incorporate environmental contexts, such as time and location.

For remote access control, a few models have been proposed [11-13], which benefit from the advantages of both RBAC and trust management systems in an open environment. In particular, the TrustBAC model [12] supports automatic user-role assignment based on not only credentials of a stranger but its past behavior and recommendations. Saffarian et al. proposed a new dynamic user-role assignment approach for remote access control [14]. It addresses the principle of least privilege without degrading the efficiency of the access control system. Moreover, it takes into account both credentials and the past behavior of the requestor in such a way that he cannot compensate for the lack of necessary credentials by having a good past behavior.

Due to the uncertainty of execution time and task allocation, the methods mentioned above cannot fit well access control in operating systems.

III. BACKGROUND CONCEPT

For most secure operating systems, user is treated as trustworthy if he passes the authentication mechanism. This principle, however, is hard to apply for current uses. In one side, hackers may obtain the authentication credence of users and login system bypassing the authentication module, obviously, these hackers cannot be regarded as trusted users. In the other side, trustworthiness is a value of experience and should differ in different authentication mechanism.

In our previous work [15], we borrowed the idea of uncertainty reasoning in expert system and proposed a reasoning model for measuring authentication trustworthiness. In this paper, we associate the authentication mechanism with access control in supporting automated role transition.

Definition 1. **Authentication Trustworthiness:** the trustworthy degree of the subject who has passed system authentication, denoted by $t_{au}(u)$. The value of $t_{au}(u)$ is between 0 and 1. The larger the value is, the more the degree of trustworthy is.

$$t_{au}(u) = p(H \mid E) \tag{1}$$

H denotes that user is trustworthy and E is the authentication mechanism. The precondition E is independent of H. When user selects a role r, the authentication trustworthiness of current role inherits that of the user, that is, $t_{au}(u) = t_{au}(r)$.

Definition 2. **Trustworthiness Increase Degree** reflects the trustworthy increase after passing the system authentication, denoted by $ASTF(H, E)$, E is the system authentication mechanism.

$$ASTF(H, E) = \begin{cases} \dfrac{p(H \mid E) - p(H)}{1 - p(H)} & p(H) < 1 \\ 0 & p(H) = 1 \end{cases} \tag{2}$$

Normally, $ASTF(H, E)$ is given by experience, with (2), we can get the Authentication Trustworthiness by (3):

$$p(H \mid E) = ASTF(H, E) + (1 - ASTF(H, E))p(H) \tag{3}$$

IV. DIVERSITY-BASED ROLE TRANSITION

In this section, we investigate a diversity-based implicit role transition method in RBAC model. As we know, explicit role transition needs user intervene thus inflexible for application, while complete implicit transition may result in privilege management out of control. In order to reduce the risk while keeping flexibility, we introduce the DRT-RBAC model, which enforce some restriction on implicit role transition. According to the strength of authentication mechanism, a range for role transition can be computed, and users whose diversity between the old role and the new one fall into this range are allowed for automated transition.

Based on DRT-RBAC model, a diversity measurement method, Debit, is further proposed for real system deployments.

 ISBN: 978-1-61208-153-3

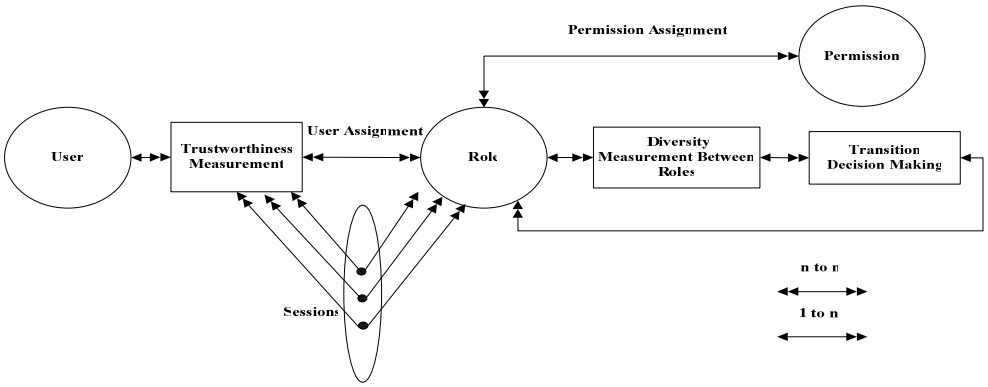

Figure 1. DRT-RBAC Model

A. *DRT-RBAC Model*

DRT-RBAC inherits basic elements from RBAC96 model and makes some extensions, as illustrate in Figure 1.

Similar to RBAC96 model, users are assigned to roles and the roles are mapped to permissions. While distinguishingly, DRT-RBAC adds a new concept of role diversity and support automated role transition. A user is usually assigned several roles in a given system, and only selects one in login. Automated role transition means a user can transit to that role implicitly if the current role of the user has no the privilege for current operation, while another available role has the corresponding privilege.

Definition 4. **Role Diversity:** the difference between roles, denoted by $d(r_1, r_2)$.

Automated role transition do not need manual intervene and largely enhance the flexibility of user operation. While unlimited transition may render system security, we enforce some restriction on automated transition, only those whose diversity between the old role and the new one fall into a transition range are allowed for automated transition. Transition range is decided on his authentication trustworthiness. Basically, the stronger the authentication mechanism, the larger the transition range. Transition threshold defines the maximum transition range. DRT-RBAC model keeps the advantage of permission management, while emphasizes on the flexibility of user-role assignment and made operating system friendly to users. Figure 2 illustrates the role transition decision process.

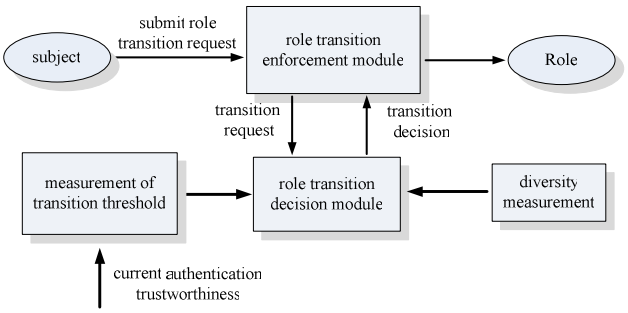

Figure 2. Role Transition Decision Process

Definition 5. **Transition threshold:** the maximum role diversity in current authentication mechanism, denoted by $d_{\max}(u)$.

Rule 1. Role transition rule: With authentication trustworthiness of $t_{au}(r_1)$, user can transit role implicitly from r_1 to r_2 if $d(r_1, r_2) < d_{\max}(u)$.

The role transition decision module is the centre part in the transition process. We will give the measurement of its input, role diversity and transition threshold, in the following sections.

B. *Debit Design*

Basically, role diversity can be measured from many aspects. In operating system, capability differentiates roles on system privilege and is a good reflector on role diversity; therefore, we proposed a capability based method named Debit to measure role diversity in this paper.

Different capabilities weigh differently since each of them has different effect on system, such as system management, security management, network management and so on. In order to measure role diversity accurately, Debit uses an analytic hierarchy process [16], in which we have two layers, capability and role. Through constructing a pair wise comparisons matrix, Debit calculates a weight for each category of capability. The diversity of two roles is finally obtained based on the weight of each capability category and the number difference of capabilities on the category.

Supposed we have k roles and n capabilities. Debit works as followed:

(1) Capability categorization

According to their function, capabilities are classified into m categories, $T_1, T_2, \ldots\ldots, T_m$, let CN_i^j be the number of T_j capabilities in $role_i$.

(2) Constructing Pair wise comparisons matrix in capability layer

TABLE I. THE FUNDAMENTAL SCALE FOR PAIR WISE COMPARISONS

Intensity of importance	Definition	Explanation
1	Equal importance	Two elements contribute equally
3	Moderate importance	Experience and judgment slightly favor one element over another
5	Strong importance	Experience and judgment strongly favor one element over another
7	Very strong importance	One element is favored very strongly over another, its dominance is demonstrated in practice

Through comparing the effect of each category on operating system, we construct a pair wise comparisons matrix. Pair wise comparing matrix reflects the intensity of importance between each pair of capability categories. The scale of the intensity is referenced from table I. The pair wise comparisons matrix of capability is shown in figure 3, a_{ii} shown is one of the value 1, 3,5,7,9 or it's reciprocal, $a_{ii}=1,\ a_{ij}=1/a_{ji}$.

(3) Checking Consistency

Debit should check the consistency of the pair wise comparisons matrix. The reason which results in the inconsistency is the improper decision of the intensity of importance between each pair of capability categories.

TABLE II. RI REFERENCED VALUE

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

Rule 2. Consistency checking rule: the pair wise comparisons matrix is consistent if $a_{ij}a_{jk}=a_{ik}$, $1 \le i, j, k \le n$ or the maximal matrix eigenvalue equal to its order.

$$V=\begin{array}{c} \\ T_1 \\ T_2 \\ \\ T_{m-1} \\ T_m \end{array}\begin{array}{c} \begin{array}{ccccc} T_1 & T_2 & \cdots & T_{m-1} & T_m \end{array} \\ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m-1} & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m-1} & a_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m-11} & a_{m-12} & \cdots & a_{m-1m-1} & a_{m-1m} \\ a_{m1} & a_{m2} & \cdots & a_{mm-1} & a_{mm} \end{bmatrix} \end{array}$$

Figure 3. Pair wise comparisons matrix of capability

Basically, incomplete consistency is acceptable in some extend. Debit uses (4) to judge whether the matrix has a satisfying consistency. If $CR < 0.1$, it's acceptable, else we should adjust the matrix V until satisfying.

$$CR = CI / RI \quad (4)$$

CI is computed through (5), and RI is obtained from table II.

$$CI = \frac{\lambda_{\max}(V)-n}{n-1} \quad (5)$$

(4) Computing weight for each category of capability

Debit computes the maximal matrix eigenvalue W, which is corresponding to the weight of each capability category.

(5) Measuring diversity for roles

In role layer, in order to measure the diversity between two roles, for example, role *a* and role *b*, we need to construct one pair wise comparisons matrix for each capability category, thus we are able to measure the difference on each capability category between role *a* and role *b*. And their diversity is finally got through the weighed summation of these differences.

For each category of capability, we construct a pair wise comparisons matrix for each pair of roles. In these matrixes, the intensity of importance is decided by their number difference of each capability category, $CN_i^h - CN_i^k$, and also referenced from table I. For role *i*, capability category *h, k,* let its matrix eigenvalue is $W_i=(b_{ih},b_{ik})$, then the diversity between role *i* and role *j* is:

$$D(R_i,R_j)=\sum_{n=1}^{m} W \times |(b_{in}-b_{jn})| \quad (6)$$

C. Transition Threshold

In this paper, we use authentication trustworthiness to get the transition threshold. Let the maximum authentication trustworthiness is 1, the transition threshold of current authentication mechanism is in proportion to the corresponding authentication trustworthiness. User who needs implicit role transition checks the diversity between two roles; and only those whose diversity between the old role and the new one fall below the threshold are allow for implicit transition.

V. IMPLEMENTATION IN CENTOS 5.4

We implement DRT-RBAC model and Debit in Centos 5.4. The kernel version is linux 2.6.18, in which we have 31 capabilities. Each bit of the low 32 bits denotes one capability and the high 32 bits are left for extension. We

TABLE III. THE $ASTF(H,E)$ UNDER DIFFERENT AUTHENTICATION MECHANISMS

authentication mechanism	$ASTF(H, E)$
password	0.1
u-key	0.3
fingerprint	0.6

 ISBN: 978-1-61208-153-3

implement three authentication mechanisms, which are password, u-key and fingerprint. Their trustworthiness increase degree is set in table III.

According to (4), we are able to get the authentication trustworthiness of each authentication mechanisms, and set it in the structure of current active task by PAM module.

We set five roles in Centos 5.4, which is system admin, security admin, audit admin, net admin and default role. The capability of each role is illustrated using hexadecimal mode in table IV. The triples represent inherit (i), permitted (p) and effective (e) capability respectively. In general, the execute capability of a process denotes the active capability, and is inherited from the inherit capability of its role. Thus we use the first element in the triples of role, inherit capability, to measure diversity between roles.

TABLE IV. CAPABILITY OF EACH ROLE

role	Capability <i,p,e>
default role	<0，0，0>
net admin	<9800feff，0，0>
system admin	<9ffffeff，0，0>
security admin	<200006，0，0>
audit admin	<60810000，0，0>

We classify the 31 capabilities into 5 categories, which is system management (SYM), security management (SEM), audit management (AUM), net management (NEM) and routine (ROU). By weighing their importance, we get the pair wise comparisons matrix of capability. Table V gives the composition of capabilities of each category in each role.

This matrix is consistent, we get the normalized maximal eigenvalue, $\boldsymbol{W}$= (0.28894, 0.28894, 0.28894, 0.0802, 0.053). This is the relative weight of all roles.

TABLE V. CAPABILITIES OF EACH CATEGORY IN EACH ROLE

role	ROU	NEM	SYM	SEM	AUM
Default role	0	0	0	0	0
net admin	11	4	0	0	0
system admin	13	4	11	0	0
security admin	2	0	1	1	0
audit admin	0	0	2	0	2

In role layer, we construct several pair wise comparison matrixes for each pair of roles. Each matrix denotes their difference on each category of capability. The intensity of importance is decided on the number difference in Table 4, and the diversity between roles is finally obtained from (6).

In the pair wise comparison matrix, the maximal intensity of importance is 7, and thus we are able to compute the maximal diversity between roles, which is 0.75. Figure 5 illustrate the transition threshold for all pairs of roles.

	AUM	SEM	SYM	NEM	
AUM	1	1	1	4	5
SEM	1	1	1	4	5
SYM	1	1	1	4	5
NEM	1/4	1/4	1/4	1	2
ROU	1/5	1/5	1/5	1/2	1

Figure 4. Pair wise comparisons matrix of capability in CentOS 5.4

I. CONCLUSION

In this paper, we propose a diversity-based access control model DRT-RBAC. DRT-RBAC support implicit role transition according to the authentication trustworthiness of users. This model keeps the advantage of permission management, while emphasizes on the flexibility of user-role assignment and made operating system friendly to users. In our future work, we will consider the temporal factor affecting the transition on roles.

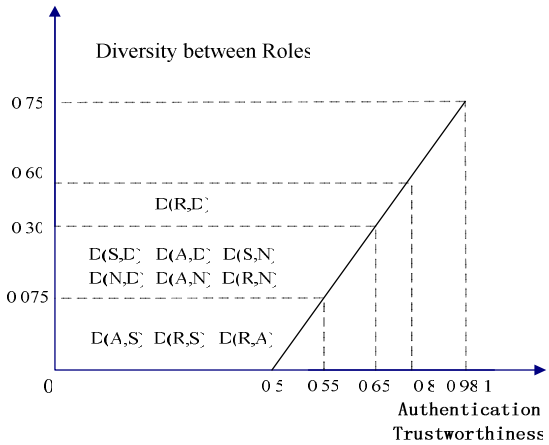

Figure 5. Transition threshold of each pair of roles

REFERENCES

[1] J. Odell, H.V.D. Parunak, S. Brueckner, and J. Sauter, "Changing Roles: Dynamic Role Assignment," Journal of Object Technology, vol 2, no 5, pp 77-86, 2003.

[2] J. Liao, X. Zhu, H. Xiao, "Separation of Duty in Dynamic Role Translations Between Administrative Domains," Journal of Computer Research and Development, pp. 43(6):1065~1070, 2006.

[3] A. Kapadia, J. Al-Muhtadi, R.H. Campbell, and M.D. Mickunas, "IRBAC 2000: Secure interoperability using dynamic role translation," In Proceedings of the 1st International Conference on Internet Computing, pp. 231-238, 2000.

[4] A. Samuel, A. Ghafoor, and E. Bertino, "A Framework for Specification and Verification of Generalized Spatio-Temporal Role-based Access Control Model," Technical report, Purdue University, CERIAS TR 2007-08, February 2007.

 ISBN: 978-1-61208-153-3

[5] V. Atluri and S.A. Chun, "A geotemporal role-based authorisation system," International Journal of Information and Computer Security, v.1 n.1/2, pp.143-168, 2007.

[6] S.M. Chandran and J.B.D. Joshi, "LoT-RBAC: A Location and Time-based RBAC Model," In Proceedings of the 6th International Conference on Web Information Systems Engineering, pp. 361-375, New York, NY, USA, November 2005.

[7] I. Ray and M. Toahchoodee, "A Spatio-Temporal Role-Based Access Control Model," In Proceedings of the 21th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, pp.211-226, Redondo Beach, CA, July 2007.

[8] E. Bertino, P.A. Bonatti, and E. Ferrari, "TRBAC: A Temporal Role-based Access Control Model," In Proceedings of the 5th ACM workshop on Role-based access control, pp.21-30, Berlin, Germany, July. 2001.

[9] J.B.D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A generalized temporal role-based access control model," IEEE Transactions on Knowledge and DataEngineering, pp.17(1):4~23, January 2005.

[10] I. Ray and M. Toahchoodee, "A Spatio-temporal Access Control Model Supporting Delegation for Pervasive Computing Applications," In Presented at Proceeding of the 5th international conference on trust, privacy and security in Digital Business, Turin, Italy, 2008.

[11] A. Herzberg, Y. Mass, J. Michaeli, Y. Ravid, and D. Naor, "Access control meets public key infrastructure, or: Assigning roles to strangers," In Proceedings of the 2000 IEEE Symposium on Security and Privacy, pp.2-9, Washington, DC,USA, 2000.

[12] S. Chakraborty and I. Ray, "TrustBAC: integrating trust relationships into the RBAC model for access control in open systems," In Proceedings of the eleventh ACM symposium on Access control models and technologies, New York, NY, USA, 2006.

[13] Y. Zhong, B. Bhargava, and M. Mahoui, "Trustworthiness based authorization on www," Department of Computer Science, Purdue University CERIAS Tech Report 2002-08, 2002.

[14] M. Saffarian, Q. Tang., W. Jonker, and P. Hartel, "Dynamic User-Role Assignment in Remote Access Control," CTIT-09-14, 2009.

[15] L. Wang, L. Wei, X. Liao, and H. Wang, "AT-RBAC: an Authentication Trustworthiness-based RBAC Model," In Proceeding of the 3rd Grid and Cooperative Computing -GCC 2004 Workshops, 2004.

[16] T.L. Saaty, "How to make a decision: the analytic hierarchy process," Interfaces, vol. 24, pp.19-27, 1994.

 ISBN: 978-1-61208-153-3