Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FUZZY IMPROVEMENTS OF CROSSING-TIMINGS INHERITANCE MECHANISM OF ROLES

[12]JIANJUN WANG, [1]JIANPING LI, [2]YONGFAN LI, [2]CHONGMING MA

[1] School of Computer Science, University of Electronic Science and Technology of China, Chengdu 610054 Sichuan, China

[2] Information Science and Technology Department, Hunan First Normal University, Changsha 410002, Hunan, China

ABSTRACT

As TRBAC is short in solving the role mutual exclusion mechanism coming from crossing-timings or overlapping-timings when roles inherited for the role authorities in distributed environments suffered temporal constraints, this paper proposes the use of susceptibility and value-at-risk for judging the degree of mutual exclusion of roles, while the relation between susceptibility and value-at-risk could be described by a Signoid function, the susceptibility of a role could be calculated by a fuzzy judgment and the comprehensive susceptibility of the inherited role across timings could be amended by Hamming Distance, and gives the inheritance algorithm which is conducive to improve the inheritance efficiency of roles restrained by tenses and example demonstrations of adjacent roles across time domains, and in the end indicates the advantages and disadvantages of the algorithms.

Keywords: *Tense, Role, Inheritance, Fuzziness, Safe*

1. INTRODUCTION

Using a role to link a subject and a object, RBAC[1] is a mainstream access control model for its flexible and convenient authority management mechanism at present. With the developments of distributed applications, such as mobile computing, the role authorities of RBAC are associated with the contexts of tense, location and so on. Literature [2] proposed to expansion the Model TRBAC on the basis of tense to realize the temporal constraints of roles; GTRBAC[3] further improved the temporal constraint mechanism of TRBAC and defined the user role assignment, role permission assignment and role inheritance relations based on the temporal constraint. Literature [4] defined GEO-RBAC by taking OGC as the location model and built the role constraint mechanism on the foundation of location information. And then people further combining both tense and location with role management, Literature[5] defined the context roles based on locations and tenses; Literature[6,7] conducted a series of research on RBAC based on locations and tenses.

Because it's easy to appear crossing and overlapping in role authorities based on tenses and locations, there will be adverse effects on role authority management and inheritance if role mutual exclusion. The r, which is a role retrained by tense of TRBAC, could be represented by a tuple <R，T>, in which R to role and T to tense (time might as well temporal interval). If there are two crossing or overlapping role tenses in role inheritance, there might be two cases: the first one is that the role of TRBAC inherited two mutually exclusive roles in authorities in the same temporal interval and the second one is that the role of TRBAC inherited two mutually exclusive roles in authorities from adjacent tenses across temporal intervals. Assume three roles, r1<R1，T1>，r2<R2，T2> and r3<R3，T3>, among which r3 inherits r1 and r2 while r1 and r2 are mutually exclusive. Figure 1 shows the first case, in which there is a partial temporal overlapping interval <t2，t3> in r1 and r2 as well as r3 inherits both r1 and r2 in <t2，t3>; And Figure 2 indicates the second case, in which t2 and t3 are the same time and temporal intervals of r1 and r2 are adjacent.

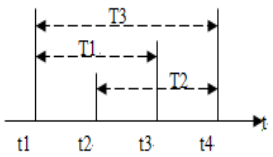

Figure 1: Mutual Exclusion Of Roles In The Same Tense

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

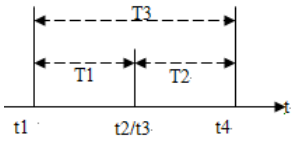

Figure 2: Mutual Exclusion Of Roles In Adjacent Tenses

"The Chinese Wall" completely isolating the security policy of object use in which there are interest conflicts in subjects' accesses, the traditional RBAC took the role mutual exclusion as a task of the complete isolation to execute, but the mechanism of that is rigid and it's hard to implement. TRBAC defined two process modes for role mutual exclusion, weak and strong process modes, in which the weak mode accepted the co-existence of mutually exclusive roles and the strong mode didn't accept the co-existence of mutually exclusive. The relation between mutually exclusive roles of TRBAC is the bounder division of authorities among roles in essence, and the two process methods, weak and strong, are the quiescent divisions for the bounders between mutually exclusive roles, but there are shortcomings in those, such as that the full containment of the weak process to mutually exclusive roles against the security of information executed by roles and that the full division of the strong process to mutually exclusive roles, which is the same as "The Chinese Wall" and the traditional RBAC, against the flexible changes of role authorities. Essentially, there are some uncertainties in mutually exclusive relations between roles, so we can consider using the fuzzy judgment to provide a dynamic evaluation for the authority inheritance relations between mutually exclusive roles.

There has been some discussions on the use the fuzzy method to improve security policies. Through the analysis of the practical applications of security mechanisms, Literature [8] improved the traditional security models with clear security bounder, proposed the point of fuzziness in security and described TCSEC model in fuzzy logic; Literature [9,10] defined relations, such as user roles, role authorities and so on, using fuzzy theory. As the aims of these literatures at static systems, stable relations of securities entities and clear bounders of securities, these fuzzy security mechanisms are not suitable for the inheritance relations of roles with crossing or overlapping timings.

According to the causes, the role mutual exclusion could be divided to timing, content and security mutual exclusions. The timing mutual exclusion means that the role has to be executed in accordance with the timing, such as doctors on day shift and night shift; content mutual exclusion means that the contents of objects are not allowed to be executed at the same time, which could be translated into timing mutual exclusion by changing executive timings. And the security mutual exclusion means there are security risks of information leakages in role objects, such as that the custom relation information of Oil Company 1 and Oil Company 2 are completely mutually exclusive, while the custom relation information of oil companies and telecommunication companies are mutually exclusive to a certain degree but not totally. The ways of information leakage could be the information random leakage, information misreading and information miswriting among roles during the executions of role authorities, etc. The strong process method proposed by TRBAC could solve the timing mutual exclusion problem, but the weak process method of that has the risk of information leakage.

Combing the fuzzy comprehensive judgment, this paper improves the inheritance mechanism of the security mutually-exclusive roles in adjacent temporal intervals, and optimizes the inheritance way of roles in continues tenses, enhancing the execution efficiency by executing the combined inheritance of roles in postorder and preorder tenses if the two roles are not mutually exclusive or are mutually exclusive within limits. Regardless of the specificity of the mutually exclusive relation between two roles for simplifying problems, this paper uses the susceptibility to describe the comprehensive judgment index of the security risk produced by the three causes, information random leakage, information misreading and information miswriting among roles, to express the security mutually-exclusive degree of roles.

2. THE FUZZY IMPROVEMENT OF INHERITANCE MECHANISM OF ROLES CROSSING TIME DOMAINS

2.1 Susceptibility and Value-at-Risk

The susceptibility shows the security mutually-exclusive degree of the object content executed by the inherited roles. And the value-at-risk shows the probability of the risk produced by roles' susceptibility, which is widely used in the analysis of risk investment, and this paper introduces it into the analysis of information security.

The relationship of susceptibility and value-at-Risk enjoys characteristics of the positive growths in value and growth rate as well as step, etc. The definitions and formalization descriptions of the positive growths in value and growth rate and step are as followings.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Assume Sen1 for the susceptibility of Role 1, Sen2 for the susceptibility of Role 2, and utilize thr to express the threshold of the value-at-risk and n for the maxlevel of susceptibility, $0 \le Sen \le n$, $0<VaR<1$, $0< thr <1$.

Positive Growth in Value: the lower susceptibility of roles, the lower value-at-risk to a user to combine inheritances to execute two roles, and vice versa, the higher susceptibility of roles, the higher value-at-risk.

Rule 1 If Sen1>Sen2，then VaR1>VaR2.

Positive Growth in the Growth Rate of Value: in unit time, the more growth in the susceptibility of roles, the more growth in the value-at-risk, what's meaning that in unit time, the value-at-risk realize the positive growth with the growth of susceptibility, and the positive growth may even be exponential growth.

Rule 2 If dSen1>dSen2，then dVaR1>dVaR2.

Step: a threshold could be set for value-at-risk, and the execution could be inherited within the threshold, otherwise the execution couldn't be inherited if beyond the threshold, which means the risk is too big.

Rule 3 If VaR<thr，inheritance will be performed；if VaR≥thr，inheritance will not be performed.

From the above three rules, the relationship between VaR and Sen could be described by a function, and Formula (1) is the relationship representation of VaR to Sen.

$$VaR=f(Sen)=\frac{1}{1+e^{-(Sen-thr)}} \qquad (1)$$

2.2 Susceptibility and Value-at-Risk

As being a multi-factors decision-making method, fuzzy comprehensive judgment could make a more comprehensive evaluation for things. According to the ways of information leakage of roles, it could define the subset of influence factor as $U=\{u_1, u_2, u_3\}$, in which u_1 for the risk of role information random leakage, u_2 for the risk of information misreading among roles, and u_3 for the risk of information miswriting among roles. The judgment set, $V=\{v_1, v_2, v_3, \ldots, v_n\}$, corresponding to the level of susceptibility expresses the security levels, and if assume that there are five levels for susceptibility then $V=\{v_1, v_2, v_3, v_4, v_5\}$, in which v_1 for higher, v_2 for high, v_3 for middle, v_4 for low, v_5 for lower. The corresponding relationship between the judgment set and susceptibility is shown in Table 1.

Table 1: The Corresponding Relationship Between Security Level And The Value Of Level

Level	Higher	High	Middle	Low	Lower
Susceptibility	5	4	3	2	1

There are m members in the project team giving risk judgments to each role, and the Table 2 shows the risk evaluation about Role R1.

Table 2: The Evaluation On Risk Factors About R1 From Evaluation Experts

U	V				
	Higher	High	Middle	Low	Lower
u_1	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
u_2	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}
u_3	C_{31}	C_{32}	C_{33}	C_{34}	C_{35}

Set $r_{ij}=\frac{c_{ij}}{k_i}$, in which $\sum_{j=1}^{5} c_{ij}=k_i, k_i \le m$, $i\in\{1, 2, 3, 4, 5\}$, $j\in\{1, 2, 3\}$

And then the judgment matrix for single factor is the Formula (2).

$$N=\begin{pmatrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ r_{31} & r_{32} & r_{33} & r_{34} & r_{35} \end{pmatrix} \qquad (2)$$

Giving the weight of $A=(a_1, a_2, a_3)$ for three factors, then the weight of each factor is determined by its influence on the susceptibility of roles, which means higher weight, the heavier influence on susceptibility. By using the model M（∧, ∨）to calculate, the comprehensive judgment result could be get as shown in the Formula (3).

$$\underset{\sim}{B}=A\circ N=(b_1, b_2, b_3, b_4, b_5) \qquad (3)$$

To set the security level corresponding to ∨{ b_1, b_2, b_3, b_4, b_5 } for the susceptibility of roles.

2.3 Susceptibility and Value-at-Risk

If a user combines and inherit two roles of Role 1 and Role 2, Sen1 and Sen2 will produce the comprehensive susceptibility Sen, and for the differences in roles the value of the comprehensive susceptibility Sen could be minimal or maximal, and the extremes only appear under the case that the two roles owning special factors. And just likes the human society, the most of the roles have common characteristics, so the value of Sen matches the normal distribution of probability density function, which Signoid function could set the value of the threshold of Sen in the center of the distribution curve by adjustments, and the Function h(Sen1,Sen2) uses a corrected value to correct Sen1 and Sen2 and takes the maximum as the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

comprehensive susceptibility. The basic idea of this algorithm is:

(1) Set the value of the threshold of susceptibility as the basic value, respectively calculate Hamming distances between the susceptibilities, Sen1 and Sen2, of two roles and the value of the threshold of susceptibility, and take the average of the two Hamming Distances as the correction value of the susceptibility of two roles.

(2) Take v{Min+Correction Value, Max-Correction} as the comprehensive Sen value for the two roles.

3. INHERITANCE ALGORITHM OF ROLES CROSSING TIME DOMAINS

This paper extends the data structure of role r to (R, T, Sen).

Sequential(Role) * The algorithm of grouping roles according to timing

{

Traverse all role sequences R[n], goto the bubble comparative calculation in accordance of timings, and build an array structure of A[i].

}

Cross_Temporal_Role_Inherite( ) * Combination Inheritance Algorithm of adjacent roles crossing time domains

{

1. Fuzzy comprehensive judgment for the susceptibilities of each role.

2. Initialization role Sequence R[n];

3. Execute Sequential(R[n]);

4. Circulate the ArrayA[i], in which 1 for the initial value for I, 2 for step-length, to the last role. Directly do the execution if only one role.

5. Execute Sen =h(Sen1,Sen2);

6. Calculate VaR=f(Sen)= $\frac{1}{1+e^{-(Sen-thr)}}$

7. To decide whether the same user could combine and inherit the execution according to the value of VaR

}

The Execution Logic Figure of Combination Inheritance Algorithm of Adjacent Roles Crossing Time Domains is as shown in Figure 4

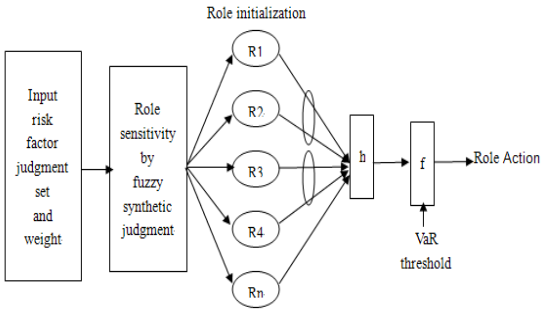

Figure 3: The Logic Figure Of The Inheritance Algorithm Of Roles Crossing Time Domains

If t for the execution time of role behavior, the continuous execution time of n roles is nt, the traversal time is n and the time complexity is (nt+n). The most ideal situation for using the inheritance algorithm of roles crossing time domains is that the adjacent roles are not mutually exclusive and each two adjacent roles could be combined and inherited to execute, in which nt/2 for the time required, n for the time required for traverse, and (nt/2+n) for the time complexity.

4. EXAMPLE DEMONSTRATIONS

Assume that a role sequence sorted by timings is （T，R_1），（T+1，R_2），（T+2，R_3），（T+3，R_4），…..，（T+n，R_{n+1}）.

There are five persons in the project team to give risk judgments to each role, and then the corresponding susceptibility of each role could be got after the fuzzy comprehensive judgment. If five roles in this sequence, their susceptibilities are (3,2,4,4,1), the threshold of risk is 0.5 ,and the corresponding susceptibility is 3.

In the first round, the first and second roles should be executed, including Sen1=3 and Sen2=2, and the calculation of compensation should be used to get the combined Sen =2.5 of this two roles, and then VaR= $\frac{1}{1+\sqrt{e}}$ < 0.5 could be calculated by substituting that into Formula (1), so this two roles could be combined and inherited by the same user.

In the second round, the third and forth roles should be executed, including Sen3=4 and Sen4=4, and the calculation of compensation should be used to get the combined Sen =4 of this two roles, and then VaR= $\frac{1}{1+e^{-(4-3)}}$ >0.5 could be calculated by substituting that into Formula (1), so this two roles couldn't be combined and inherited by the same user.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the third round, we should execute the fifth role, but for there is only one role, so we can directly substitute it into the Formula (1), and get $VaR=\frac{1}{1+e^{-(1-3)}} < 0.5$, so the executions could be inherited.

From experiences, we could also obtain that the risk of combining and inheriting the executions of the first and second roles is lower, that of the third and forth roles is higher, and the fifth role could be inherited executions separately, which matches the judgment result of the above calculation.

5. CONCLUSION

There are four advantages in the fuzzy improvement scheme proposed by this paper for timing role inheritance mechanism. The first one is that to combine and inherit executions benefits the improvement of the execution efficiency of role sequences, and there are more demands for it in businesses processed according to the flows, such as auditing service, accounting business, and accesses of mobile nodes to resources according to timings, etc; and the second one is that there are two dynamic decision points in fuzzy comprehensive judgment scheme, dynamics in the risk judgment and the weight sets for risk factors, which could dynamically change the susceptibility of roles and influence the authority inheritances and execution sequences of roles to increase the flexibility of the executions of roles, such as a director of the hospital has two roles of the manager and doctor, but this two roles are mutually exclusive, and if the doctor role should be executed in the manager temporal interval in case of emergence, the executions of this two roles could be combined and inherited by changing the susceptibilities to reduce the degree of mutual exclusion; and the third one is that the fuzzy judgment scheme for security proposed for combining and inheriting executions of two roles could efficiently improve the comprehensive security of executions of roles; and the last one is that the role which is added susceptibility constraint has no constraints on some mechanisms of TRBAC, such as task dissociation, permission allocation and so on, the reason of which is that these mechanisms doesn't involve the problem of mutual exclusion among roles, so increasing constraints on the susceptibility of roles couldn't improve the complexities of these mechanism.

This paper discusses the combination and inheritance cases of each two adjacent roles, as well as the deficiencies in Zadeh operator, judgments needed by roles and the lacks of consideration for the extreme cases are the disadvantages of this paper. At last, it will be the content for the next work that how to solve the security problem of combining and inheriting executions of multi roles in the same timing and the security problem of combining and inheriting executions of roles in nonadjacent temporal intervals.

ACKNOWLEDGEMENTS

This paper is supported by Aid program for Science and Technology Innovative Research Team in Higher Educational Institutions of Hunan Province(2010-212), A Project Supported by Scientific Research Fund of Hunan Provincial Education Department (10C0528)

REFERENCES:

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-Based Access Control Models", *IEEE Computer*, Vol. 29, No. 2, 1996, pp. 38-47.

[2] E. Bertino, P.A. Bonatti, and E. Ferrari, "TRBAC: A Temporal Role-Based Access Control Model," *ACM Trans. Information and System Security*, Vol. 4, No. 3, 2001, pp. 191-233.

[3] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 17, No. 1, 2005, pp. 4–23.

[4] E. Bertino, B. Catania, M. L. Damiani, P. Perlasca, "GEO-RBAC: a spatially aware RBAC", Proceedings of the 10th ACM Symposium on Access Control Models and Technologies, ACM Press, June 01-03, 2005, pp. 29–37.

[5] S. M. Chandran, J. B. D. Joshi, "LoT-RBAC: A Location and Time-Based RBAC Model", Proceedings of the 6th international conference on Web Information Systems Engineering, Springer Press, November 20-22, 2005, pp. 361–375.

[6] I. Ray, M. Toahchoodee, "A Spatio-Temporal Role-Based Access Control Model", Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Springer Press, July 8-11, 2007, pp. 211–226.

[7] M. Toahchoodee, I. Ray, "On the Formal Analysis of a Spatio-temporal Role-Based Access Control Model", Proceedings of the 22st Annual IFIP WG 11.3 Working Conference on Data and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Applications Security, Springer Press, July 13-16, 2008, pp. 17–32.

[8] H. H. Hosmer, "Using Fuzzy Logic to Represent Security Policies in the Multipolicy Paradigm", ACM SIGSAC Reviews, ACM Press, October 15, 1993, pp.175-184.

[9] H. Takabi, M. Amini, "Separation of Duty in Role-Based Access Control Model through Fuzzy Relation", Third International Symposium on Information Assurance and Security, IEEE CS press, August 29-31, 2007, pp.125-130.

[10] U.H.G.R.D Nawarathna, S.R. Kodithuwakku, "A Fuzzy Role Based Access Control Model for Database Security", Proceedings of the International Conference on Information and Automation, December 15-18, 2005, pp.313-318.