Accepted Manuscript

Supporting user authorization queries in RBAC systems by role-permission reassignment

Jianfeng Lu, Yun Xin, Zhao Zhang, Hao Peng, Jianmin Han

PII: S0167-739X(17)32443-3
DOI: https://doi.org/10.1016/j.future.2018.01.010
Reference: FUTURE 3917

To appear in: *Future Generation Computer Systems*

Received date : 30 October 2017
Revised date : 23 December 2017
Accepted date : 3 January 2018

Please cite this article as: J. Lu, Y. Xin, Z. Zhang, H. Peng, J. Han, Supporting user authorization queries in RBAC systems by role-permission reassignment, *Future Generation Computer Systems* (2018), https://doi.org/10.1016/j.future.2018.01.010

Supporting User Authorization Queries in RBAC Systems by Role-Permission Reassignment

Jianfeng Lu[a,b,*], Yun Xin[a], Zhao Zhang[a], Hao Peng[a], Jianmin Han[a]

[a] *Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, Zhejiang, China*
[b] *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, Jiangsu, China*

Abstract

The *User Authorization Query* (UAQ) Problem is a key issue related to efficient handling of users' access requests in *Role Based Access Control* (RBAC) systems. However, there may not exist any solution to a given UAQ problem due to the limitation caused by the current system state, because missing any requested permission may thwart a task, while an extra permission may bring an intolerable risk to the system. Hence, update of the role-permission assignment is needed to support the feasibility of an UAQ problem. In this paper, we study fundamental problems related to role-permission reassignment, including the RVP problem the goal of which is to determine whether a given role-permission assignment satisfies all reassignment objectives and does not violate any prerequisite constraint or permission-capacity constraint, the RFP problem which verifies whether there exists a valid role-permission assignment, and the RGP problem which studies how to generate a valid role-permission assignment. We present the computational complexity analysis of RVP, RFP and RGP, showing that RVP is solvable in linear time, while both RFP and RGP are NP-hard. We also propose an approach for RGP, which incorporates a preprocessing to decrease the size of the problem, and reduce it to an SAT problem. Finally, experimental results show the validity and effectiveness of our proposed approach.

Keywords: user authorization query, role based access control, role-permission reassignment, computational complexity, SAT problem

1. Introduction

Role based access control (RBAC) has received considerable attention over the past two decades, and established itself as a predominant model for advanced access control in many organizations and enterprises [1]. Several beneficial features, such as policy neutrality, support for least privilege, and efficient self-management, are associated with RBAC models. Such features make RBAC suitable for handling access control requirements of diverse organizations [2, 3]. A fundamental problem in RBAC is to determine whether there exists an optimum set of roles whose activation can provide a specific set of permissions requested by a user. This is introduced as the user authorization query (UAQ) problem by Y. Zhang et al [4]. UAQ has been the subject of considerable researches in recent years, and widely accepted as a key issue related to efficient handing of users' access requests in RBAC [5, 6, 7, 8, 9, 10, 11].

Ideally, the chosen set of roles to be activated needs to satisfy the user's requested permissions exactly. However, this is not always possible. Hence we have to find a set of roles whose activation can provide a set of permissions that is as close as possible to the set of permissions requested by a user. Motivated by such a consideration, G. T. Wickramaarachchi et al. [5] studied the UAQ problem with a lower bound and an upper bound for the set of requested permissions. There are two optimization objectives for the UAQ problem. One is to minimize the number of extra permissions, which is motivated by the principle of least privilege [12], because too many extra permissions may bring intolerable risks to the system. The other is to minimize the number of missing permissions, because the unavailability of too many requested permissions may make it difficult for a user to carry out his required task. Existing approaches to the UAQ problem primarily focus on how to design approximate or exhaustive solutions [5, 6, 7, 11]. However, a feasible solution for UAQ may not exist since it is possible that no combination of roles can collectively activate only the requested permissions in a given interval.

The reason why there does not exist any solution for a given UAQ problem is the limitation caused by the current system state. Hence, a novel approach for the UAQ problem by making some changes of an RBAC state is desirable. In general, an RBAC state describes the set of permissions for which a role is assigned, and a user can acquire associated permissions via roles to take the associated tasks, that is to say, it is determined by three types of assignment relations: *user-role* assignment relation (UA), *role-role* assignment relation (RH), and *permission-role* assignment relation (PA) [1, 13]. J. Hu et al. [14] refer to the updating of UA, RH and PA in the role maintenance stage as *role updating*. Observe that, UA is business-driven, users' role memberships are determined by their attributes, such as jobs, titles, etc. Hence, in this paper, we focus on the update of RH and PA. It should be noted that role hierarchy plays a crucial role in policy specification and se-

*Corresponding author. E-mail: lujianfeng@zjnu.cn.