COMPUTERS & SECURITY 60 (2016) 79–94

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Mining temporal roles using many-valued concepts

Barsha Mitra [a], *Shamik Sural* [a], *Jaideep Vaidya* [b,*], *Vijayalakshmi Atluri* [b]

[a] *Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India*
[b] *Management Science and Information Systems Department, Rutgers University, USA*

ARTICLE INFO

Article history:
Received 21 July 2015
Received in revised form 18 March 2016
Accepted 6 April 2016
Available online 11 April 2016

Keywords:
TRBAC
Temporal role mining
Many-valued concept
Matrix decomposition
Access control

ABSTRACT

Many of today's access control policies are associated with temporal restrictions. Under temporal role-based access control (TRBAC), roles have an associated temporal component, which allows them to better encapsulate such temporal access control policies. However, given their complexity, TRBAC systems can only be well managed if the set of roles is correctly defined. The process of deriving an optimal set of such roles is known as temporal role mining. In this paper, we formally define the temporal role mining problem (TRMP) in the form of a matrix decomposition problem, by introducing a new operator that multiplies a set with a Boolean value and redefining existing matrix multiplication operations in terms of it. We also define a new metric for temporal role mining, called cumulative overhead of temporal roles and permissions (CO-TRAP), which takes into consideration the administrative effort required for managing the resulting TRBAC system. Since TRMP as well as minimization of CO-TRAP are NP-complete problems, we propose two greedy algorithms based on many-valued concepts. Experimental evaluation on a number of real-world datasets shows that the proposed approach is both efficient and effective.

1. Introduction

Ensuring authorized access to system resources is one of the major concerns of system administrators. In order to achieve this, several access control models have been proposed. role-based access control (RBAC) (Sandhu et al., 1996) is one such model. In an RBAC system, users acquire permissions through a set of roles assigned to them. To effectively deploy an RBAC system, these roles need to be properly defined. This process of role definition, known as role engineering, may be carried out in two ways – *top-down* (Neumann and Strembeck, 2002; Roeckle et al., 2000) and *bottom-up* (Lu et al., 2008; Molloy et al., 2008; Vaidya et al., 2006). The top-down approach requires manual inspection and understanding of the business processes whereas the bottom-up approach can be automated to a significant extent, and semantically augmented with human expertise. Role mining is one such bottom-up approach to role engineering. It derives a set of roles, a user-role assignment (UA) relation describing the set of roles assigned to each user and a role-permission assignment (PA) relation indicating the set of permissions present in each role from direct user-permission assignments, if already available with the organization.

Many of today's organizational access control policies restrict access to resources for selective durations of time. RBAC

* *Corresponding author.*
E-mail addresses: barsha.mitra@sit.iitkgp.ernet.in (B. Mitra), shamik@sit.iitkgp.ernet.in (S. Sural), jsvaidya@business.rutgers.edu (J. Vaidya), atluri@rutgers.edu (V. Atluri).
http://dx.doi.org/10.1016/j.cose.2016.04.002
0167-4048/

cannot be deployed in such scenarios since no temporal constraint is associated with the roles. In order to provide a means for such access control in terms of roles, a number of temporal extensions such as the temporal role-based access control (TRBAC) model (Bertino et al., 2001) and the generalized temporal role-based access control (GTRBAC) model (Joshi et al., 2005) have been proposed. In TRBAC, a role is enabled for a specific time duration, during which a user can assume that role and acquire the permissions associated with it. The time duration for which a role is available to a user is specified in a *role enabling base* (REB). Therefore, in addition to a UA and a PA, an REB also needs to be derived through role mining for implementing a TRBAC system. However, existing role mining approaches do not consider any form of temporal information associated with user-permission assignments while deriving the roles. In order to overcome this shortcoming, very recently, two temporal role mining techniques (Mitra et al., 2013, 2015) have been proposed. Such mined roles have an associated temporal component. In the rest of the paper, we refer to them as *temporal roles*.

The problem of mining a minimal set of temporal roles from the given temporal user-permission assignments is known as the temporal role mining problem (TRMP). TRMP was informally introduced in Mitra et al. (2013) and later extended in Mitra et al. (2015) as the generalized temporal role mining problem (GTRMP). TRMP aims to generate a *consistent* solution while GTRMP allows a limited amount of inconsistency as well. However, no mathematical formulation for TRMP in terms of the notion of consistency exists in the current literature.

In this paper, we present a mathematical formulation for TRMP in terms of matrix decomposition. To this end, we introduce a new operator which we call the *Boolean-set multiplication* operator that multiplies a set with a Boolean value. A greedy heuristic based on many-valued concepts (Encheva, 2012; Messai et al., 2008, 2010) is then proposed for solving TRMP.

While minimization of the total number of roles can produce a fully functional TRBAC system, it does not capture the unique characteristics of TRBAC that distinguish it from an RBAC system. Moreover, mere minimization of the number of roles does not fully represent the overall administrative effort required to manage the complete system. To address this issue, we propose a new minimization metric for temporal role mining, which we name as the *cumulative overhead of temporal roles and permissions* (CO-TRAP). This metric is expressed as the weighted sum of the sizes of the REB and the PA relation. CO-TRAP captures the overhead of creating, storing and maintaining the roles in a TRBAC system by incorporating both the temporal overhead (in terms of the REB size) and the permission overhead (in terms of the size of the PA). We name the problem that minimizes this metric as the *cumulative overhead of temporal roles and permissions minimization problem* (CO-TRAPMP). A greedy algorithm using the notion of many-valued concepts is also proposed.

The rest of the paper is organized as follows. Some preliminaries related to TRBAC and temporal role mining are discussed in Section 2. Section 3 introduces the new multiplication operator, defines three existing matrix products in terms of this operator, and presents a mathematical formulation of TRMP using the proposed operator and matrix products. In Section 4, a greedy matrix decomposition algorithm based on many-valued concepts for solving TRMP is described. The metric CO-TRAP and the corresponding temporal role mining problem CO-TRAPMP along with its solution strategy are presented in Section 5. Experimental evaluation of both the proposed approaches is discussed in Section 6. Section 7 reviews existing work on both non-temporal and temporal role mining. Finally, Section 8 concludes the paper and provides directions for future research.

2. Background

We now provide a brief overview of TRBAC and temporal role mining.

2.1. Temporal role-based access control (TRBAC)

TRBAC (Bertino et al., 2001) is an extension of the RBAC model. It restricts the set of time intervals during which a role can be enabled. For the rest of the time, the role remains disabled. The set of time intervals during which a role can be enabled or disabled is specified in a role enabling base (REB) and is expressed as $\langle [begin, end], P \rangle$, where P is a periodic expression denoting an infinite set of periodic time intervals, while *begin* and *end* are date expressions, respectively, imposing lower and upper bounds on the set of time intervals represented by P. Each periodic expression is expressed in terms of a set of *Calendars*, each of which in turn denotes a set of consecutive time intervals. Calendars can be of different granularity such as, *Years*, *Months*, *Weeks*, *Days* and *Hours*. Enabling or disabling of a role r is expressed using an event expression of the form *enable* r or *disable* r along with the corresponding periodic expression denoting the set of time intervals during which this event is to occur.

2.2. Temporal role mining

A user-permission assignment relation that captures the time duration for which the permissions are available to the users is known as a temporal user-permission assignment relation. As per Mitra et al. (2013), such a relation can be represented using a temporal UPA (TUPA) matrix. The rows and columns of TUPA correspond to users and permissions, respectively. If user i is assigned permission j for a set T_{ij} of time intervals, then entry (i, j) of TUPA, $\text{TUPA}_{ij} = T_{ij}$, otherwise, $\text{TUPA}_{ij} = \phi$. Moreover, T_{ij} can represent a continuous set of time intervals implying that permission j is always assigned to user i. Though assigning a permission to a user for an unrestricted time duration essentially means that no temporal constraint is associated with the permission assignment; however, a constraint of the form $all.Years + all.Days + \{0\}.Hours \triangleright 24.Hours$ needs to be specified to signify the presence of this assignment in the TUPA (since a null value would indicate that the assignment is not possible). The process of deriving a set of roles R, a UA, a PA and an REB from a TUPA is known as temporal role mining (Mitra et al., 2013).