A Case Study on the Suitability of Process Mining to Produce Current-State RBAC Models

Maria Leitner

Stefanie Rinderle-Ma

RG Workflow Systems and Technology
University of Vienna

Anne Baumgraß

Sigrid Schefer-Wenzl

Mark Strembeck

Institute for Information Systems
Vienna University of Economics and Business (WU Vienna)

SBP'12, September 3th 2012

Introduction

Process Mining techniques

- analyze and extract process-related information from event logs
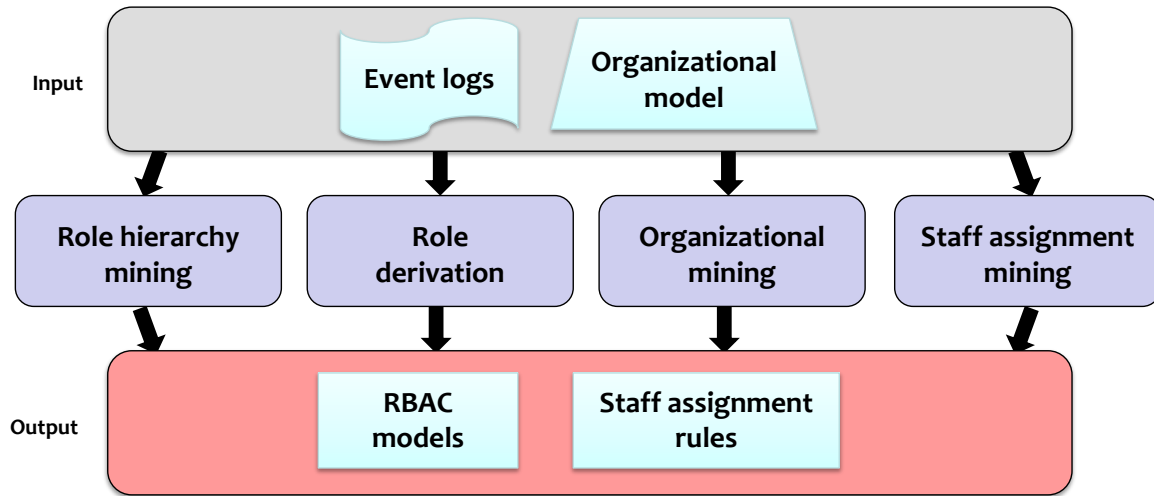- do not directly focus on the derivation of current-state RBAC models

Role-based access control (RBAC) as de facto standard for access control in research and industry

Vision: To examine, analyze and use existing mining techniques to derive RBAC models

Goal: Give initial guidance on which of these approaches can be applied in which particular context and which prerequisites are necessary

This paper: Investigates the applicability of four approaches to extract current-state RBAC information from event logs
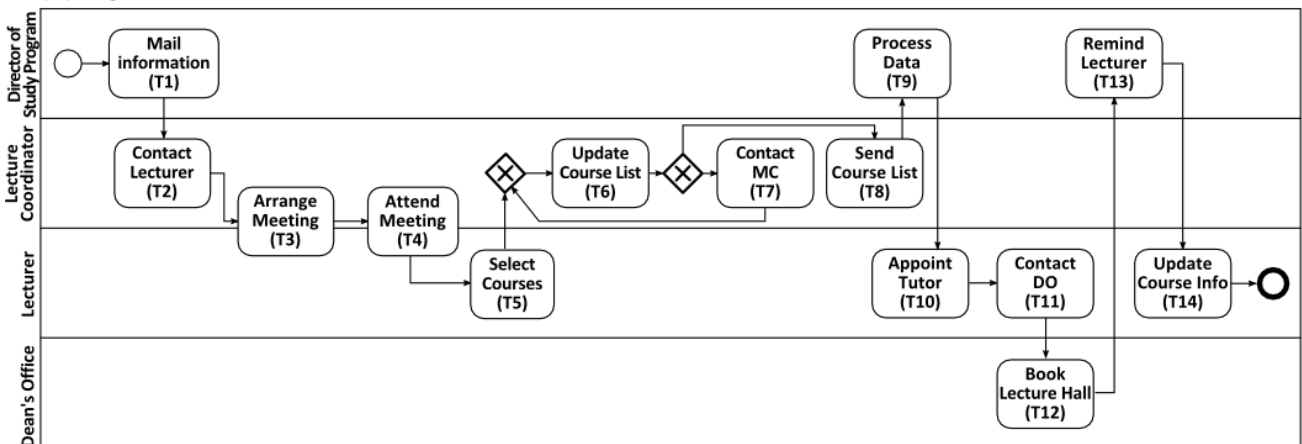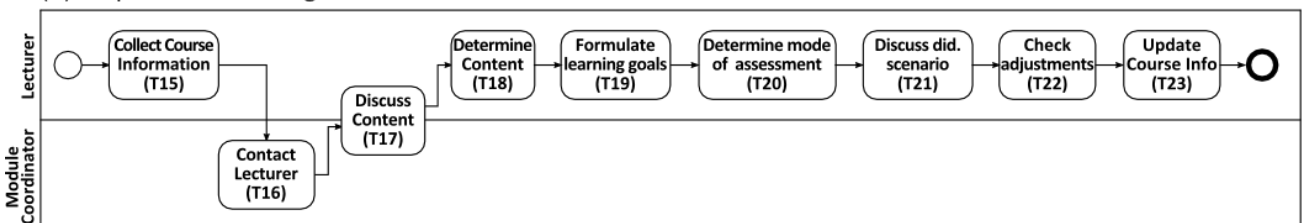
Problem Statement

Input

| Event logs | Organizational model |

| Role hierarchy mining | Role derivation | Organizational mining | Staff assignment mining |

Output

| RBAC models | Staff assignment rules |

➜ Guidance for selecting approaches for current-state RBAC models

Case Study – Use Case from Academia

(A) Organization of Lectures
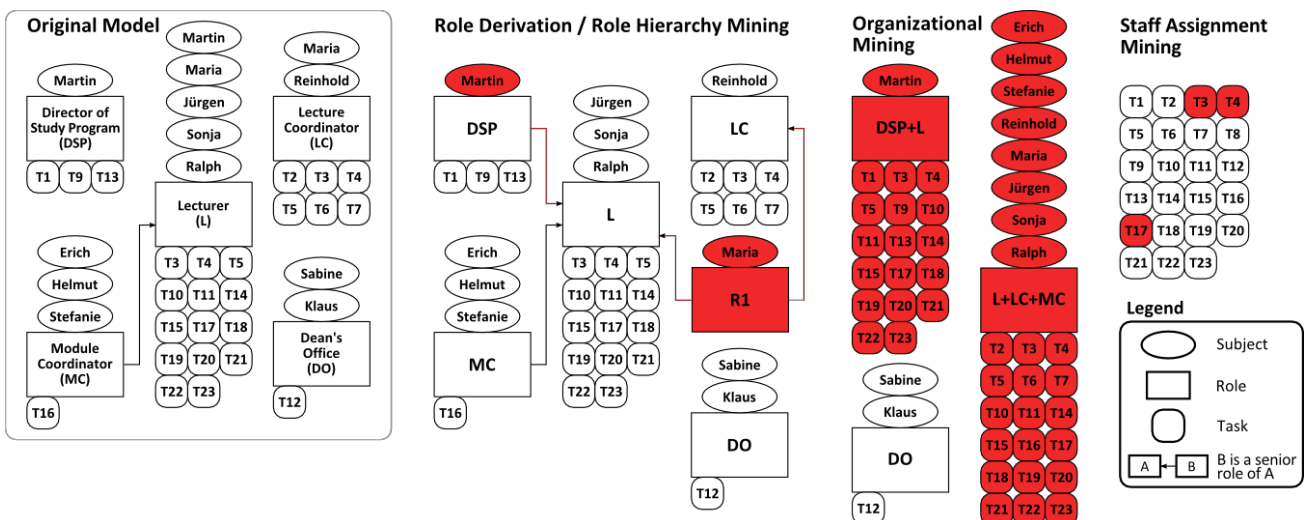

(B) Prepare Course Design

Case Study - Approach

- Process from Higher Education System
  - 23 tasks
  - 5 process-relevant roles
- Used CPN Tools to generate event log with 100 cases
  - 11 subjects performing tasks in cases

Application in:

- ProM 5.2
  - Role hierarchy
  - Organizational mining (Social network mining)
  - Staff assignment mining
- xoRET
  - Role derivation

Results - Models

Results - Quantitative Measurements

	Original Model	Role Derivation	Role Hierarchy	Staff Assignment	Organizational Mining
Characteristics					
Roles	10 (5 relevant)	6	6	-	3
Organizational Units	11 (2 relevant)	-	-	-	-
Role-to-Subject Assignments	13	11	11	-	11
Task-to-Role Assignments	25	25	25	23	36
Comparison to Original Model					
Roles exactly identified	-	5	5	-	1
Role-to-Subject Assignments	-	11	11	-	11
Task-to-Role Assignments*	-	25	25	20**	1
Accuracy (acc)	-	100%	100%	-	20%
Coverage (cov)	-	100%	100%	80%	4%

* covered by discovered (exactly identified) roles
** staff assignment rules matched by (exactly identified) task-to-role assignments

$$acc = \frac{\text{no. of roles identified exactly}}{\text{no. of roles in original model}}$$

$$cov = \frac{\text{no. task-to-role assignments covered by discovered roles}}{\text{no. task-to-role assignments in original model}}$$

Zhang et al: Permission Set Mining: Discovering Practical and Useful Roles. In: Proc. of the 2008 ACSAC. IEEE (2008)

Evaluation and Discussion

Role derivation and **role hierarchy mining** have the highest coverage and accuracy

Organizational mining requires a certain amount of domain knowledge

Staff assignment mining suitable for task-to-role assignments

Factors in the Evaluation:
- Discovering original roles
- Unidentified roles
- Frequency of executions

Conclusion and Future Work

Initial guidance for selecting approaches to derive current-state RBAC models

Role derivation and **role hierarchy** were the most suitable techniques to derive current-state RBAC models

Future Work:

Enhancing the use case: process and organizational model

Expand our tests to different domains

Determine if we obtain similar results