Analyzing Quality Criteria in Role-based Identity and Access Management

Michael Kunz[1], Ludwig Fuchs[1,2], Michael Netter[1,2] and Günther Pernul[1]
[1]*University of Regensburg, Regensburg, Germany*
[2]*Nexis GmbH, Münster, Germany*
firstname.lastname@wiwi.uni-regensburg.de

Keywords: Role Quality, Role Mining, RBAC, Identity and Access Management.

Abstract: Roles have turned into the de facto standard for access control in enterprise identity management systems. However, as roles evolve over time, companies struggle to develop and maintain a consistent role model. Up to now, the core challenge of measuring the current quality of a role model and selecting criteria for its optimization remains unsolved. In this paper, we conduct a survey of existing role mining techniques and identify quality criteria inherently used by these approaches. This guides organizations during the selection of a role mining technique that matches their company-specific quality preferences. Moreover, our analysis aims to stimulate the research community to integrate quality metrics in future role mining approaches.

1 INTRODUCTION

Regulating access to resources is an elementary function of every identity management system (IdMS). Not just as a result of governmental regulations or compliance requirements like the Sarbanes-Oxley Act ((SOX, 2002)), Basel III ((Basel Comittee on Banking Supervisions, 2010)), or the EU General Data Protection Regulation ((European Union, 2012)) in its revised form, especially medium- and large-sized companies are forced to control access to sensitive information. Over the past decades, Role-Based Access Control (RBAC, (Sandhu et al., 1996)), has become the de facto standard for managing access to resources in IT systems. In RBAC, roles act as intermediary between users and permissions. Despite being widely used, RBAC struggles with the dynamic evolution of role models over time. Besides the daily user administration, the central challenge after setting up a role model is its strategic maintenance. Role system maintenance focuses on updating and cleansing role configurations, discarding unused, and defining new roles. Changing business processes, organizational structures, or security policies and newly imposed regulations force administrators to quickly adapt the access control structures in place. Commonly, this leads to an increasing role number, an overall reduction of the role model quality and the advent of security vulnerabilities due to wrongly assigned or outdated role definitions.

In order to mitigate the risk of increasing security vulnerabilities in RBAC, one cornerstone of ensuring a high role model quality is the periodic assessment of the role model components, such as the user-role assignments (*UA*), the role-permission assignments (*RA*), or role hierarchy structures. Role mining approaches that support organizations during their initial setup of an RBAC model have attracted the attention of researchers. Over the last four years, for instance, a variety of research groups have published approaches to generate an initial set of roles. However hardly any attention has been drawn to the maintenance of existing role models. Recently, the need for investigating and cleaning role model structures has been highlighted by (Fuchs et al., 2014). However, the core challenge of measuring the current quality of a role model and selecting criteria for its optimization still remains unsolved. Due to its importance for access control it is likely that role mining is re-applied periodically by organizations in order to ensure role model correctness. Our work builds on both, the in-depth investigation of the research area as well as our practical experience from industry projects within medium- and large-sized companies dealing with the setup and management of a role-based IdMS. Similar to (Fuchs et al., 2014), we argue that the practical project requirements cannot be considered to a sufficient extent by the available role mining approaches. In particular, we address the following research question (RQ): *Which quality criteria are employed in ex-*

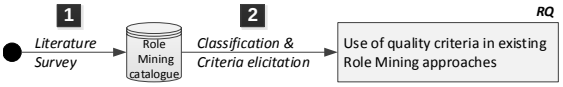

Figure 1: Research methodology.

isting role mining approaches?

Hence, the contribution of this work is twofold. In order to close the existing research gap, this paper firstly analyzes the development of role mining, presenting a survey of the field and underlining the rapid development in the area. In this respect, it builds on an existing survey of the area published in the year 2011. During execution, various role mining algorithms rely on some sort of quality criteria to different extents. As a result, this paper secondly extracts potential criteria for rating the quality of role models included in current role mining approaches. It points out the differences among the approaches and underlines the need for a structured quality rating process. We thereby aim at stimulating the research community and encourage them to enrich existing role mining approaches considering quality criteria in a structured manner.

2 RELATED WORK

In todays medium- and large-sized companies, Role-based Access Control has become the de facto standard for controlling user access to resources. As a result of the large amount of research output, several surveys of the general area of roles in IT security have been presented (e.g. (Zhu and Zhou, 2008) and (Fuchs et al., 2011)). Authors lately agreed upon the growing importance of role development in general and automated role mining in specific. Fuchs et al., for instance, provided an evaluation of role development approaches in (Fuchs and Müller, 2009) and (Fuchs and Meier, 2011). Since their publication, the research output in the area has grown more than double, requiring a survey update in order to give an in-depth understanding of recent developments.

During the initial setup of a role model, role mining algorithms inherently rely on different quality criteria to various extents. Nevertheless, no structured analysis considering those criteria has been executed so far. It has rather been shown that popular role mining approaches like (Molloy et al., 2010), (Giblin et al., 2010), or (Takabi and Joshi, 2010) do not offer the guidance required to judge the correctness of role definitions and role models (Fuchs et al., 2014). In practice, however, it is very likely that companies reapply role mining techniques in order to ensure role model correctness after having employed a role mining approach for the initial role setup. Yet, none of the related work in the field focuses on quality criteria applied during role system maintenance. In (Molloy et al., 2008), the authors investigated the usage of selected metrics like the Weighted Structural Complexity (WSC) for analyzing role system states. (Fuchs and Müller, 2009) described mechanisms for periodically evaluating a role systems quality but do not consider the scalability of their approach in large real-world scenarios. (Fuchs et al., 2014) recently proposed the integration of a distinct quality rating and role classification phase in their role optimization process model. However, they do not present an overview of available quality criteria and their application. As a result, the core challenge of measuring the current quality of a role model still remains unsolved.

3 METHODOLOGY

Our methodology to answer the research questions presented in Section 1 is depicted in Figure 1. At first, we survey the research area and create a catalog of role mining approaches that serves as the basis for further analyses (step 1). For this literature survey, we follow the methodology proposed by (Levy and Ellis, 2006). We carried out a bibliographic database search including the ACM Digital Library, DBLP, IEEE Digital Library, and Google Scholar using the keyword ”role mining”. To arrive at a complete catalog of role mining approaches, author and reference search for each publication was applied to identify previously undiscovered research. Finally, papers that do not present role mining techniques were removed from the catalog (e.g. (Molloy et al., 2008)). Consecutively, we classify recent role mining publications according to the scheme presented by (Fuchs and Meier, 2011). Additional clusters were added for role mining approaches that used new techniques. Note, that approaches that rely on more than one role mining technique were clustered based on the predominant technique being used. At this stage we completed our first contribution by extending the existing survey and highlighting the rapid increase of research within the last three years as well as the further diversification of role mining techniques used. During step 2 of our methodology we answer RQ by investigating the usage of quality criteria in role mining algorithms.

4 ROLE MINING SURVEY

This section extends a survey on role mining research conducted by (Fuchs and Meier, 2011). Figure 2 un-

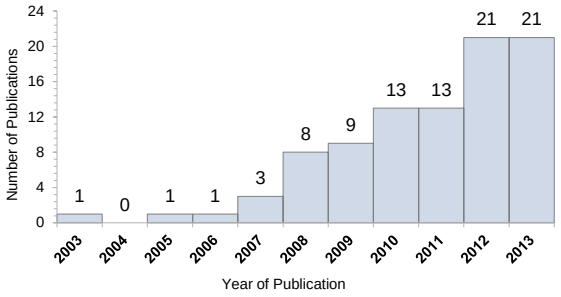

Figure 2: Development of the research area.

derlines the importance of an updated interpretation of role detection approaches due to the increase in researchers' attention during the last three years. Between 2011 and 2013, 55 papers related to role mining have been published, representing an increase of 141 percent compared to the number of publications from 2003 - 2010 (39). While role mining in general consists of a pre-processing phase, a role detection phase, and a post-processing phase (Fuchs and Meier, 2011), the remainder of this survey focuses on the role detection phase as the core element of every role mining algorithm. During this phase, suitable roles are created based on an existing set of user-permission assignments (*UPA*). The algorithms can be grouped according to the underlying technique. While the first six techniques have been previously introduced in (Fuchs and Meier, 2011), we identified three additional techniques (Visual Role Mining, Boolean Matrix Decomposition, and Attribute-based Role Mining) being applied to solve the role mining problem for the first time. Additionally to the 21 algorithms published in (Fuchs and Meier, 2011), 26 out of the 55 approaches from 2011 to 2013 have been categorized, while the rest is related to either pre- or post-processing phase. Subsequently, each technique and representative publications are presented:

Subset Enumeration aims to discover roles through creating all possible intersections of permission sets. Due to the exponential complexity of enumerating all possible subsets, algorithms such as (Xu and Stoller, 2013b) use heuristics for role candidate selection. Hence, role mining algorithms based on this technique strive to balance complexity and quality of results. With 13 available algorithms, this is the most frequently used technique in role mining.

Clustering is a role mining approach that is directly derived from data mining (Frank et al., 2012). Using a *UPA*-matrix as input, this technique searches for clusters with similar permissions. However, clustering approaches struggle with limitations such as requiring users or permissions to be only part of one single cluster (Frank et al., 2012). To solve these challenges, several clustering variants exist. Examples include iterative application of the technique or reduction of the input (Lu et al., 2013; Huang et al., 2012).

Graph Optimization uses bipartite graphs to represent the *UPA* (Colantonio et al., 2009). As roles represent an intermediary between the two disjoint vertices of users and permissions, those approaches aim at converting the bipartite into a tripartite graph or a representation with sub-graphs. Roles are then represented by the middle vertex (Colantonio et al., 2009) or each necessary sub-graph (Mandala et al., 2012).

Frequent Permission Set Mining has its roots in marketing analysis and algorithms of generic frequent set mining (Agrawal et al., 1993). Initially used for the study of consumers' purchase behavior, it is applied by role mining algorithms in order to discover permissions that frequently occur together. The presumption is that permission sets that appear together can be interpreted as role candidates.

Formal Concept Analysis is a data mining technique similar to clustering, overcoming the limitation of only assigning entities to one group (Molloy et al., 2008). Related algorithms build a concept lattice from the *UPA*-matrix and reduce duplicate information. A concept lattice is a construct similar to a graph and represents roles and their connection in a partially ordered collection of clusters which again consist of permissions and users.

Heuristic Matrix Selection is similar to Subset Enumeration without the initial role set being based on intersections of permissions. Instead, it iterates through rows (or columns) and picks role candidates successively according to the highest number of given assignments (e.g permissions assigned to a user). Initially, each row/column is treated as a role. Subsequently, a cross-check for duplicate roles is conducted (Blundo and Cimato, 2010).

Visual Role Mining is a fairly new technique initially proposed in (Colantonio et al., 2012). It reorders rows and columns of the input *UPA*-matrix in order to create clusters of adjoined permissions. Displayed to an administrator, the underlying assumption is that humans' cognitive capabilities and context knowledge are better suited to discover proper roles compared to purely algorithm-based approaches.

Boolean Matrix Decomposition is an approach that directly addresses the Role Mining Problem (RMP) introduced by (Vaidya et al., 2007). This formal definition of role mining and targets at decomposing the boolean *UPA*-matrix into two separate matrices, a *UA*-matrix and a *PA*-matrix. By dividing the initial *UPA*-matrix into two consistent sub-matrices, the columns of the *UA*-matrix and the rows of the *PA*-matrix build up the set of roles.

Attribute-based Role Mining such as (Frank et al., 2009) are trying to incorporate business information through attributes into role mining. They rely on the assumption that additional semantic data is available and can be taken into account. Attribute-based approaches combine other techniques and enrich them with attribute-based mechanisms to arrive at an improved role set.

5 QUALITY-RELATED CRITERIA

After their classification we examined role mining algorithms regarding their decision making processes of including certain role candidates in their final output. We argue that this central decision making provides well-suited indicators for quality management in RBAC. This assumption is based on the claims of several publications (e.g. (Xu and Stoller, 2012), (Zhang et al., 2013b)) of outperforming competitive approaches in terms of the quality of generated roles. A total of 23 different quality criteria can be identified. They either focus on the quality of the overall RBAC state, the quality of single roles, or both. At first we focus on RBAC state quality criteria. Secondly, we examine criteria that deal with the quality of an individual role (cf. Table 1). Note that for some criteria (e.g. *Exclude Unused Permissions*) additional input information is required. In the following, we present a detailed interpretation of the quality criteria and group them according to their focus.

Achieve Completeness. Completeness refers to the exact representation of the original access control state, i.e. the goal is to cover the initial UPA-matrix with the resulting set of roles. In contrast to most approaches (e.g. (Zhang et al., 2007; Vaidya et al., 2006; Blundo and Cimato, 2010)), some techniques allow to deviate to a certain extent from the initial UPA-matrix based on a given threshold (the so called $\delta - RMP$ (Vaidya et al., 2007))(Chu et al., 2012; Lu et al., 2008). Completeness therefore measures the quality of a RBAC state by measuring the degree to which a resulting role set represents the initial access control situation.

Reduce Number of Roles. Initially formulated in the RMP, the goal of having as few roles as possible is based on the assumption that complexity of RBAC is directly connected to the number of roles maintained. Thus, the number of roles in a given RBAC state is a quality criteria usable to rate the estimated administrative efforts to manage the role model. Depending on the size of a company in terms of its employees, permissions and UPA, this measure can be normalized in order to allow for a comparison of role models in different organizations.

Decrease Role Set Similarity. Quality criteria related to Role Set Similarity measure the distance between two given sets of roles. They are mainly used for the measurement of the dissimilarity of RBAC states (e.g. in (Zhang et al., 2013a)) or the difference between a current RBAC state and a targeted state. In (Jafari et al., 2009), for instance, the permission similarity is measured using the Euclidean Distance. Furthermore, the Jaccard Similarity is a popular metric used in a variety of approaches (Mandala et al., 2012; Xu and Stoller, 2013a; Chu et al., 2012).

Minimize Users/Permissions per Role & Minimize/Maximize Roles per User/Permission. Quality criteria assigned to this category target at two main objectives. First, the definition of an upper bound per role limiting the amount of users assigned to one role. Second, the objective of finding as few as possible permissions that are placed in a role. This can, for instance, be applied in case an organization aims at defining a larger number of small roles for employees that exactly fit their specialist tasks. On the contrary, maximizing the number of users or permissions per role can be beneficial other scenarios, e.g. when organizations aim at defining a small set of large roles. Moreover, Minimizing/Maximizing the roles per element (user or permission) is applied in seven existing role mining approaches (e.g. see (Lu et al., 2013; Ma et al., 2013)). This can be useful in order to minimize the role model complexity in terms of relationships among the role model elements.

Fullfill Role Constraints. Role Constraints impose restrictions on the definition of roles. For instance, (Ma et al., 2012) consider Segregation of Duty (SOD) policies that entail mutually exclusive permissions in the RBAC state. Other policies, such as the four-eye-principle, that affect the user assignments of a role are also conceivable.

Reduce WSC. In contrast to most other quality criteria the so called Weighted Structural Complexity (WSC) is a widely-used heuristic to rate the complexity of a RBAC model. Originally introduced by (Molloy et al., 2008), it applies weights to different optimization objectives. It can be seen as one of the most advanced measures that solely relies on the components of an RBAC state. It is usable for both, individual roles and role sets, and thus allows for a good

Table 1: Quality Criteria in existing approaches.

Technique / Focus	Paper	State			Individual Role							State + Individual Role											
		Achieve Completeness	Reduce Number of Roles	Decrease Role Set Similarity	Minimize Users per Role	Maximize Users per Role	Minimize Roles per User	Minimize Roles per Permission	Minimize Permissions per Role	Maximize Permissions per Role	Fulfill Role Constraints	Reduce WSC	Optimize Matrix Sorting	Decrease Permission Similarity	Reduce Role Redundancy	Increase User Similarity	Decrease Permission Attr. Sim.	Increase Role Coverage	Exclude Unused Permissions	Consider Timestamp	Consider Role Attributes	Consider User Attributes	Group by Attributes
Subset Enumeration	(Chu et al., 2012)	■	■			■								■	■								
	(Colantonio et al., 2008a)	■	■			■				■		■											
	(Huang et al., 2012)	■	■			■				■								■					
	(Lu et al., 2013)	■	■				■			■								■					
	(Mitra et al., 2013)	■	■																	■			
	(Molloy et al., 2012)	■	■															■	■				
	(Vaidya et al., 2006)	■	■			■																	
	(Vaidya et al., 2007)	■	■															■					
	(Vaidya et al., 2010b)	■	■				■			■								■					
	(Vaidya et al., 2010a)	■	■																				
	(Xu and Stoller, 2012)	■								■		■			■			■				■	
	(Xu and Stoller, 2013b)	■										■						■					
	(Zhang et al., 2013a)	■		■	■												■						
Clustering	(Frank et al., 2008)	■	■				■									■							
	(Frank et al., 2012)	■																					
	(Frank et al., 2013)	■															■				■		
	(Kumar et al., 2011)	■							■														
	(Schlegelmilch and Steffens, 2005)	■	■																				
Graph Optimization	(Colantonio et al., 2009)	■	■																				
	(Colantonio et al., 2010)	■	■																				
	(Ene et al., 2008)	■	■		■				■														
	(Gal-Oz et al., 2011)	■													■				■				
	(Hingankar and Sural, 2011)	■	■		■																		
	(Mandala et al., 2012)	■		■	■														■				
	(Zhang et al., 2007)	■										■											
Frequent Permission Set Mining	(Colantonio et al., 2008b)	■	■											■									
	(Jafari et al., 2009)			■										■				■	■				
	(Ma et al., 2010)	■										■		■		■							
	(Ma et al., 2012)	■			■		■				■												
	(Ma et al., 2013)	■	■					■											■				
	(Zhang et al., 2008)	■																■					
Formal Concept Analysis	(Molloy et al., 2008)	■																					
	(Wang et al., 2012)	■	■																				
	(Wong et al., 2012)	■	■															■					
Heuristic Matrix Selection	(Blundo and Cimato, 2010)	■	■																				
	(Blundo and Cimato, 2013)	■			■				■	■	■												
	(Huang et al., 2010)	■	■			■				■													
Visual Role Mining	(Colantonio et al., 2012)	■	■										■					■					
	(Eucharista, 2013)	■	■									■	■					■					
Boolean Matrix Decomposition	(John et al., 2012)	■	■				■																
	(Lu et al., 2012)	■	■																				
	(Lu et al., 2008)	■	■																				
	(Uzun et al., 2011)	■	■																				
	(Ye et al., 2013)	■	■									■											
Attribute-based Approaches	(Frank et al., 2009)	■	■																				■
	(Han et al., 2012)	■																					■
	(Li et al., 2012)	■					■																■

Uses criteria: ■ Yes □ No

comparability of RBAC states. As a result of its popularity, several existing role mining approaches are able to consider the WSC.

Optimize Matrix Sorting. Matrix sorting aims at covering an initial access control state by sorting the input UPA-matrix based on user accounts with similar permissions and permissions that are assigned a similar set of user accounts. (Colantonio et al., 2012) introduced the ADVISER and EXTRACT algorithms that generate a matrix representation of the initial UPA-matrix that clusters permissions and user accounts together. As a result, large areas covering initial UPA can be visually detected by a human role engineer.

Similarities & Redundancy. Well-known similarity metrics can be applied to the various elements of a RBAC state in order to measure its quality. (Takabi and Joshi, 2010) gives an overview of possible applications of the Jaccard Similarity in the context of role management. He discusses three similarity metrics that can be applied on the assignment types of a role (user, permission and role hierarchy). They can further be used to compute the similarity of two role sets (cf. Decrease Role Set Similarity). Besides examining the similarity of assignment types of a role, similarity metrics are applied to attributes of role compo-

nents. They can, for instance, be used to create a role set based on the location attribute of all user accounts. Distance measures are applied to identify redundant roles (Chu et al., 2012).

Increase Role Coverage. The Role Coverage is formally defined in (Zhang et al., 2008) as the fraction of role-covered UPA by the initial UPA. Companies aim at achieving a high role coverage in order to foster the benefits of RBAC compared to other access control models. The implication of reducing administrative costs through RBAC is represented through this criterion.

Attribute-related Criteria. Attribute-related criteria evaluate the quality of a role based on its attributes or attributes of its components. Permission usage derived from access logs, for example, can be used to display the actual usage of privileges by employees. It offer insights into unused PA that can potentially be removed during the next refinement of a role (Molloy et al., 2012). Furthermore, restrictions on the composition of a role, e.g. by allowing only certain attributes of users in a role are possible (Xu and Stoller, 2012).

6 DISCUSSION

This work is motivated by the gap between the recent uprising of role mining and the practical need for periodic quality assessment of the resulting role models. The presented survey underlined the significant growth (141%) of published papers in the recent past. We have shown that every role mining approach relies on one or more quality criteria, mostly implicitly without providing a structured integration of quality management. In the following we present a short discussion of our quality-related findings from Table 1.

Firstly, it can be seen that the main quality criterion in role mining is to arrive at an exact representation of existing access control states. This criterion is – to a varying extent – considered by all available approaches, except for (Jafari et al., 2009) which derive the roles solely from access history logs. Secondly, Table 1 shows that a large number of approaches focus on generating as few roles as possible (**Reduce Number of Roles**). Interestingly, as the WSC is a potential criterion which is able to represent this and other measures (by modifying its weight factors), recent approaches try to use this metric as a heuristic for producing high quality roles (Xu and Stoller, 2013b; Eucharista, 2013; Ye et al., 2013). This can be interpreted as an indicator that research is already trying to integrate sophisticated measures into role mining.

Other interesting results are, that criteria with practical relevance up to now are only considered by few existing approaches. Timestamps as an attribute of permissions are, for instance, only considered by one approach (Mitra et al., 2013). However, their integration into role mining seems promising as they heavily can influence role design. Sets of permissions activated together within a certain period of time can e.g. represent good candidate permissions for a role. We furthermore noted that several quality criteria well-known in practice have not yet been included in any role mining approach at all. This includes criteria like the maximum allowed number of roles in a role model, role usage or hierarchy restrictions. It seems straightforward to integrate a maximum threshold of roles to be found through automatic role discovery in order to ensure the maintainability of the whole role set. Intuitively, result sets can always be limited by just taking the desired number of roles after sorting them according to a predefined criterion. Furthermore, the usage of UA over a certain period of time (i.e. the activation of roles) can hint at outdated role definitions. Several approaches are able to take existing roles into consideration (e.g. (Molloy et al., 2008)) but do not integrate usage data. Moreover, restrictions on the hierarchy of a RBAC state can represent one way to reduce complexity and increase the quality of either a single role or the whole RBAC state. In practice, deployed RBAC states feature unlimited depth, sometimes even resulting in hierarchy loops. Limiting the maximum allowed number of parent or child roles of a role or the maximal hierarchy depth can ease administrative staff's understanding of the overall role model. Several post-processing approaches already outline the need for an inspection of the role hierarchy (e.g. (Guo et al., 2008; Takabi and Joshi, 2010)). Yet, they focus on removing duplicate hierarchy depiction and finding minimal hierarchical assignments, not on cardinality restrictions.

7 CONCLUSION

Role-Based Access Control as the de facto standard for managing access privileges in organizations struggles with the dynamic evolution of role models over time. As a result the quality of RBAC states initially modeled using role mining techniques decreases over time. In order to address this challenge, role mining mechanisms applied during role system maintenance need to be extended in order to integrate a dedicated quality management stage for rating and improving a role system state on the basis of company-specific quality criteria. In this paper we presented two con-

tributions in that respect. We firstly provided a survey giving an overview of current role mining approaches. The significant increase of research activity and the growing number of applied techniques for generating roles during the last three years underlines the relevance and diversification of the area. By extracting criteria that are dedicated to improving role quality from currently available role mining approaches we were able to answer the research question stated in Section 1. We have shown on which quality criteria current role mining approaches rely and revealed a number of practically relevant but yet untreated criteria in research. The integration of quality mechanisms in order to allow for an improved selection of role mining approaches in a given scenario based on company-specific quality criteria.

ACKNOWLEDGEMENTS

The research leading to these results was supported by the "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association. This work would not have been possible without our student Christian Wawarta.

REFERENCES

Agrawal, R., Imieliński, T., and Swami, A. (1993). Mining association rules between sets of items in large databases. In *SIGMOD Record*, volume 22, pages 207–216. ACM.

Basel Comittee on Banking Supervisions (2010). Basel III: Int. framework for liquidity risk measurement, standards and monitoring.

Blundo, C. and Cimato, S. (2010). A simple role mining algorithm. In *Proc. of the 2010 Symp. on Applied Computing*. ACM.

Blundo, C. and Cimato, S. (2013). Constrained role mining. In *6th Int. Workshop on Security and Trust Management*, pages 289–304. Springer.

Chu, V. W., Wong, R. K., and Chi, C.-H. (2012). Overfitting and error detection for online role mining. *Int. Journal of Web Services Research*, 9(4):1–23.

Colantonio, A., Di Pietro, R., and Ocello, A. (2008a). A cost-driven approach to role engineering. In *Proc. of the 2008 Symp. on Applied Computing*. ACM.

Colantonio, A., Di Pietro, R., and Ocello, A. (2008b). Leveraging lattices to improve role mining. In *Proc. of The IFIP TC 11 23rd Int. Information Security Conf.* Springer.

Colantonio, A., Di Pietro, R., Ocello, A., and Verde, N. V. (2009). A probabilistic bound on the basic role mining problem and its applications. In *Emerging Challenges for Security, Privacy and Trust*, pages 376–386. Springer.

Colantonio, A., Di Pietro, R., Ocello, A., and Verde, N. V. (2010). Taming role mining complexity in rbac. *Computers & Security*, 29(5):548–564.

Colantonio, A., Di Pietro, R., Ocello, A., and Verde, N. V. (2012). Visual role mining: A picture is worth a thousand roles. *IEEE Transactions on Knowledge and Data Engineering*, 24(6):1120–1133.

Ene, A., Horne, W., Milosavljevic, N., Rao, P., Schreiber, R., and Tarjan, R. E. (2008). Fast exact and heuristic methods for role minimization problems. In *Proc. of the 13th Symp. on Access Control Models and Technologies*. ACM.

Eucharista, A.and Haribaskar, K. (2013). Visual elicitation of roles: using a hybrid approach. *Oriental Journal of Computer Science & Technology*, 6(1):103–110.

European Union (2012). General data protection regulation.

Frank, M., Basin, D., and Buhmann, J. M. (2008). A class of probabilistic models for role engineering. In *Proc. of the 15th ACM Conf. on Computer and Communications Security*. ACM.

Frank, M., Buhman, J. M., and Basin, D. (2013). Role mining with probabilistic models. *ACM Transactions on Information and System Security*, 15(4):15:1–15:28.

Frank, M., Streich, A. P., Basin, D., and Buhmann, J. M. (2009). A probabilistic approach to hybrid role mining. In *Proc. of the 16th ACM Conf. on Computer and communications security*, pages 101–111. ACM.

Frank, M., Streich, A. P., Basin, D., and Buhmann, J. M. (2012). Multi-assignment clustering for boolean data. *Journal of Machine Learning Research*, 13(1):459–489.

Fuchs, L., Kunz, M., and Pernul, G. (2014). Role model optimization for secure role-based identity management. In *Proc. of the 22nd European Conf. on Information Systems*.

Fuchs, L. and Meier, S. (2011). The role mining process model - underlining the need for a comprehensive research perspective. In *Proc. of the 6th Int. Conf. on Availability, Reliability and Security*. IEEE.

Fuchs, L. and Müller, C. (2009). Automating periodic role-checks: A tool-based approach. In *Business Services: Konzepte, Technologien, Anwendungen: 9. Int.e Tagung Wirtschaftsinformatik*, volume 246. OCG, Wien.

Fuchs, L., Pernul, G., and Sandhu, R. (2011). Roles in information security–a survey and classification of the research area. *Computers & Security*, 30(8):748–769.

Gal-Oz, N., Gonen, Y., Yahalom, R., Gudes, E., Rozenberg, B., and Shmueli, E. (2011). Mining roles from web application usage patterns. In *Trust, Privacy and Security in Digital Business*, volume 6863 of *Lecture Notes in Computer Science*, pages 125–137. Springe.

Giblin, C., Graf, M., Karjoth, G., Wespi, A., Molloy, I., Lobo, J., and Calo, S. B. (2010). Towards an integrated approach to role engineering. In *SafeConfig*, pages 63–70. ACM.

Guo, Q., Vaidya, J., and Atluri, V. (2008). The role hierarchy mining problem: Discovery of optimal role hierarchies. In *Computer Security Applications Conf.* IEEE.

Han, D.-j., Zhuo, H.-k., Xia, L.-t., and Li, L. (2012). Permission and role automatic assigning of user in role-based access control. *Journal of Central South University*, 19:1049–1056.

Hingankar, M. and Sural, S. (2011). Towards role mining with restricted user-role assignment. In *2nd Int. Conf. on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology*.

Huang, C., Sun, J.-l., Wang, X.-y., and Si, Y.-j. (2010). Minimal role mining method for web service composition. *Journal of Zhejiang University SCIENCE C*, 11(5):328–339.

Huang, H., Shang, F., and Zhang, J. (2012). Approximation algorithms for minimizing the number of roles and administrative assignments in rbac. In *36th Annual Computer Software and Applications Conf. Workshops*. IEEE.

Jafari, M., Chinaei, A., Barker, K., and Fathian, M. (2009). Role mining in access history logs. *Journal of Information Assurance and Security*, 38.

John, J., Sural, S., Atluri, V., and Vaidya, J. (2012). Role mining under role-usage cardinality constraint. In *Information Security and Privacy Research*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 150–161. Springer.

Kumar, R., Sural, S., and Gupta, A. (2011). Mining rbac roles under cardinality constraint. In *Information Systems Security*, pages 171–185. Springer.

Levy, Y. and Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science Journal*, 9:181–212.

Li, R., Wang, W., Ma, X., Gu, X., and Wen, K. (2012). Mining roles using attributes of permissions. *Int. Journal of Innovative Computing, Information and Control*, 8(11):7909–7924.

Lu, H., Hong, Y., Yang, Y., Duan, L., and Badar, N. (2013). Towards user-oriented rbac model. In *Data and Applications Security and Privacy XXVII*, volume 7964 of *Lecture Notes in Computer Science*, pages 81–96. Springer.

Lu, H., Vaidya, J., and Atluri, V. (2008). Optimal boolean matrix decomposition: Application to role engineering. In *Proc. of the 24th IEEE Int. Conf. on Data Engineering*. IEEE.

Lu, H., Vaidya, J., Atluri, V., and Hong, Y. (2012). Constraint-aware role mining via extended boolean matrix decomposition. *IEEE Transactions on Dependable and Secure Computing*, 9(5):655–669.

Ma, X., Li, R., and Lu, Z. (2010). Role mining based on weights. In *Proc. of the 15th Symp. on Access Control Models and Technologies*. ACM.

Ma, X., Li, R., Lu, Z., and Wang, W. (2012). Mining constraints in role-based access control. *Mathematical and Computer Modelling*, 55(1):87–96.

Ma, X., Tian, Y., Zhao, L., and Li, R. (2013). Mining role based on ranks. *ICIC Express Letters. Part B, Applications: an Int. Journal of Research and Surveys*, 4(2):319–326.

Mandala, S., Vukovic, M., Laredo, J., Ruan, Y., and Hernandez, M. (2012). Hybrid role mining for security service solution. In *Proc. of the 9th Int. Conf. on Services Computing*. IEEE.

Mitra, B., Sural, S., Atluri, V., and Vaidya, J. (2013). Toward mining of temporal roles. In *Data and Applications Security and Privacy XXVII*, volume 7964 of *Lecture Notes in Computer Science*, pages 65–80. Springer.

Molloy, I., Chen, H., Li, T., Wang, Q., Li, N., Bertino, E., Calo, S., and Lobo, J. (2008). Mining roles with semantic meanings. In *Proc. of the 13th Symp. on Access Control Models and Technologies*. ACM.

Molloy, I., Chen, H., Li, T., Wang, Q., Li, N., Bertino, E., Calo, S., and Lobo, J. (2010). Mining roles with multiple objectives. In *ACM Transactions on Information and System Security*. ACM.

Molloy, I., Park, Y., and Chari, S. (2012). Generative models for access control policies: Applications to role mining over logs with attribution. In *Proc. of the 17th Symp. on Access Control Models and Technologies*. ACM.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2):38–47.

Schlegelmilch, J. and Steffens, U. (2005). Role mining with orca. In *Proc. of the 10th Symp. on AccessControl Models and Technologies*. ACM.

SOX (2002). Sarbanes-oxley act of 2002, pl 107-204, 116 stat 745.

Takabi, H. and Joshi, J. B. (2010). Stateminer: An efficient similarity-based approach for optimal mining of role hierarchy. In *Proc. of the 15th Symp. on Access Control Models and Technologies*. ACM.

Uzun, E., Atluri, V., Lu, H., and Vaidya, J. (2011). An optimization model for the extended role mining problem. In *Data and Applications Security and Privacy XXV*, pages 76–89. Springer.

Vaidya, J., Atluri, V., and Guo, Q. (2007). The role mining problem: finding a minimal descriptive set of roles. In *Proc. of the 12th Symp. on Access Control models and Technologies*. ACM.

Vaidya, J., Atluri, V., and Guo, Q. (2010a). The role mining problem: A formal perspective. *ACM Transactions on Information and System Security*, 13(3):27.

Vaidya, J., Atluri, V., and Warner, J. (2006). Roleminer: Mining roles using subset enumeration. In *Proc. of the 13th ACM Conf. on Computer and Communications Security*. ACM.

Vaidya, J., Atluri, V., Warner, J., and Guo, Q. (2010b). Role engineering via prioritized subset enumeration. *IEEE Transactions on Dependable and Secure Computing*, 7(3):300–314.

Wang, J., Zeng, C., He, C., Hong, L., Zhou, L., Wong, R. K., and Tian, J. (2012). Context-aware role mining for mobile service recommendation. In *Proc. of the 27th Annual Symp. on Applied Computing*. ACM.

Wong, R. K., Chu, V. W., Hao, T., and Wang, J. (2012). Context-aware service recommendation for moving

connected devices. In *Int. Conf. on Connected Vehicles and Expo*.

Xu, Z. and Stoller, S. D. (2012). Algorithms for mining meaningful roles.

Xu, Z. and Stoller, S. D. (2013a). Mining attribute-based access control policies from rbac policies.

Xu, Z. and Stoller, S. D. (2013b). Mining parameterized role-based policies.

Ye, W., Li, R., and Li, H. (2013). Role mining using boolean matrix decomposition with hierarchy.

Zhang, D., Ramamohanarao, K., and Ebringer, T. (2007). Role engineering using graph optimisation.

Zhang, D., Ramamohanarao, K., Ebringer, T., and Yann, T. (2008). Permission set mining: Discovering practical and useful roles.

Zhang, W., Chen, Y., Gunter, C., Liebovitz, D., and Malin, B. (2013a). Evolving role definitions through permission invocation patterns.

Zhang, X., Han, W., Fang, Z., Yin, Y., and Mustafa, H. (2013b). Role mining algorithm evaluation and improvement in large volume android applications.

Zhu, H. and Zhou, M. (2008). Roles in information systems: A survey. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, 38(3):377–396.