2013

Managing the Access Grid - A Process View to Minimize Insider Misuse Risks

Stefan Meier
University of Regensburg, Department of Information Systems, Regensburg, Germany, stefan.meier@ur.de

Ludwig Fuchs
Nexis GmbH, Regensburg, Germany, Ludwig.Fuchs@nexis-secure.de

Günther Pernul
University of Regensburg, Department of Information Systems, Regensburg, Germany, guenther.pernul@ur.de

Managing the Access Grid - A Process View to Minimize Insider Misuse Risks

Stefan Meier[1], Ludwig Fuchs[2], and Günther Pernul[1]

[1] University of Regensburg, Department of Information Systems, Regensburg, Germany
{stefan.meier,guenther.pernul}@ur.de
[2] Nexis GmbH, Regensburg, Germany
Ludwig.Fuchs@nexis-secure.de

Abstract. It is generally agreed upon the fact that the quality of Identity- and Access Management (IAM) data such as user accounts, access privileges or consistent user representation among different security domains is low. Growing user populations in medium- and large-sized organizations lead to a so called "identity chaos" in which over-privileged employees increase the risk of insider misuse. Recent governance and compliance mandates have amplified the importance of minimizing these risks. In order to fulfill these requirements, organizations focus on implementing role-based user management. To set up a role-based access control system, they face the challenge of modeling suitable roles for their employees. In this paper we show how the role modeling process can be improved by utilizing the so called access grid, a visualization technique to incorporate human interaction into the process of role creation.

Keywords: Insider Misuse, Visual Role Mining, Role Mining, Role Development, Identity Management

1 Introduction

Effectively administrating employees' access to sensitive applications and data is one of the biggest security challenges for today's organizations. A typical medium-sized or large enterprise manages millions of user access privileges[1] that are spread across thousands of IT resources. Job and position changes of employees further complicate the task of correctly managing users and their access rights. Major security problems arise because of manual management of user accounts spread across various applications. As a result, employees accumulate excessive entitlements over time. This accumulation violates the principle of the Least Privilege and increases the risk of insider threats. A study investigating industry espionage across several organizations recently underlined the importance of insider threats, revealing that confidential information is mostly stolen by internal employees and not by external attackers [1]. Addi-

[1] In the remainder, the terms permissions, entitlements and access privileges are used interchangeably

11th International Conference on Wirtschaftsinformatik,
27th February – 01st March 2013, Leipzig, Germany

tionally, compliance considerations emphasized the need for centralized, automated and secure management of employees and their access privileges. Cleven and Winter [2] state that regulations like the Sarbanes-Oxley Act of 2002 (SOX) [3] or Basel III [4] lead to an increased importance of secure IAM. Organizations need to be able to verify and prove evidence that user's access privileges conform to regulatory and corporate guidelines. In order to regain the control of the managed digital identities and their entitlements, companies aim at migrating from identity-based towards role-based user management in which identities are no longer directly related to access privileges but via roles acting as intermediary between identities and entitlements. The so called Role-based Access Control (RBAC) paradigm simplifies user management, reduces administrative costs and increases the overall security level [5-6].

In order to gain the benefits of RBAC, companies are forced to initially model a set of valid business roles for their employees. Role modeling is a task commonly executed by IT experts in cooperation with business representatives like departmental managers. The human interpretation of potential role candidates therefore represents a critical process step during role modeling. Thus, supporting the human interactor during his tasks is mandatory for successful role definition. Recently, the Role-Mining Process Model (RMPM) has been proposed, integrating the necessary steps for role creation into a process-oriented framework [7]. To increase the applicability of the RMPM and to overcome drawbacks of existing role modeling approaches, we propose the usage of the so called access grid. We show how the access grid can be facilitated in order to reduce potential insider misuse risks and define high-quality business roles in a process-oriented fashion.

This paper is structured as follows: Section 2 presents related work while Section 3 investigates visualization techniques in order to choose the grid-based visualization as the basis for the access grid. In Section 4 the integration of the access grid into the RMPM is shown. Our approach is then evaluated in Section 5 using a real-world case study. Finally, Section 6 concludes our findings and reveals future research directions.

2 Related Work

The different aspects of insider threats have been discussed by various authors, e.g. Probst et al. [8], analyzing the detection and mitigation of insider threats. Closely related, aspects of compliance in the information systems discipline have been discussed by Cleven and Winter in [2]. The authors give an overview of compliance needs and regulations and underline how the growing number of regulations and laws affects businesses. Furthermore, the need for additional research, especially on the development of new concepts and solutions to achieve compliance, is pointed out.

Implementing role-based user management conforming to the RBAC standard is commonly seen as a main element of compliant IAM and thus for minimizing insider threats. To complete the initial task of role definition, three main approaches have been proposed: Role engineering, role mining and a hybrid combination of both techniques [9]. Role engineering can be considered as the mainly manual approach, modeling roles top-down on the basis of employees' job descriptions, business processes

and organizational structuring. Neumann and Strembeck, e.g., focus on scenario-driven role engineering [10]. Role mining, on the contrary, represents the tool-based approach to identify clusters of similar users bottom-up on the basis of the existing access privilege assignments using data mining techniques. Lately, researchers have agreed upon the fact that only a hybrid combination of those two approaches leads to an applicable role catalogue in the context of enterprise-wide IAM [9].

The RMPM offers an incremental and iterative approach for hybrid role definition using role engineering as well as role mining techniques (see Figure 1). It splits the role mining tasks pre-processing (data cleansing and data selection), role detection and post-processing (integration of business semantics and hierarchy optimization) activities [7]. Role engineering results like e.g. existing work profiles or job descriptions of employees can act as input data for role mining while at the same time role mining output feeds into a new role engineering iteration.

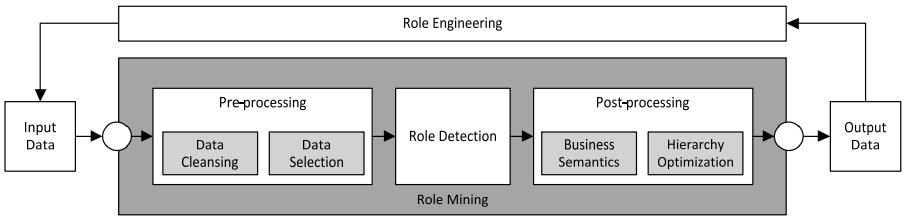


Fig. 1. The Role-Mining Process Model [7]

Several researchers already underlined the importance of data visualization during role mining. In [11], e.g., a two-dimensional matrix is facilitated to picture potential roles generated by a role mining algorithm. In other work, Zhang et al. suggest the use of a two-dimensional matrix for displaying similarities between users based on their permissions and indicating the quality of a current RBAC state [12]. Further visualizations were proposed in [9] and [12].

However, looking at the different role mining approaches underlines, that none of the current solutions provides a consistent visual component supporting the human interactor, commonly an IT-related role developer, during the process of role modeling. Existing solutions mainly concentrate on one single task or parts of the role mining activities respectively. The RMPM as the first comprehensive role modeling process integrates the single activities into a structured approach, but does not focus on the presentation and interpretation of partial results by a human. In this paper we thus focus on the role developer's tasks during the various RMPM activities. The overall goal is supporting his decision making process.

3 Visualizing Identity and Access Data

The previous section revealed the importance of information visualization in the context of role modeling and insider threat detection. In order to support a human interactor during his tasks, visualizations have to fulfill certain requirements. Their

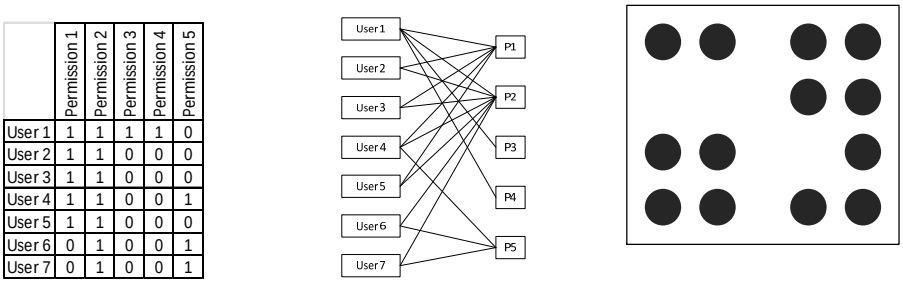
main goal is the appropriate picturing of the aggregated or non-aggregated information depending on the current activity. In the following, we present different visualization techniques and evaluate them shortly using a set of core requirements defined below. Note that the given list is not exhaustive but rather represents the most important requirements depending on literature research and practical experience.

- Scalability: Visualizations used during role modeling have to be capable of representing large datasets containing of potentially thousands of users, permissions and permission assignments.
- Perceptibility: Visualized identity-related data needs to be interpreted intuitively by a role developer. He needs, in particular, to be able to identify patterns like role candidates as well as outliers or potential errors within the given data.
- Aggregation Level: Identity-related data needs to be visualized on various aggregation levels. Aggregated information gives an overview of the underlying data structures while at the same time the role developer might need to drill down in order to gather detailed information about the displayed employee- and permission data.
- Consistency: A suitable visualization technique should be applicable during all RMPM activities. This leads to an increased user experience and simplifies the iterative comparison and communication of results.

3.1 Visualization Techniques

In the following we focus on the evaluation of common visualization techniques in order to rate their applicability during the RMPM. A comprehensive overview of basic and advanced visualization techniques is given in [13]. Due to space constraints we excluded generally unsuited visualization techniques like glyphs and icons [14], pixel techniques or bar charts and histograms in the following [13]. They lack scalability and are not capable of intuitively displaying relationships between entities like employees and their permissions. Due to the resulting low perceptibility and scalability they are not applicable consistently within the RMPM.

Table Visualizations. Table visualizations (Figure 2a) are used to display two entities and the relations between them in table cells [13]. They are capable of representing large amounts of data, increasing their scalability, mainly through the flat representation of the data. However, table visualizations are not able to provide an easily understandable and aggregated overview of the data. As they display the relationship between employees and permissions using binary values (either a 0 or 1), they struggle with a low perceptibility. A table visualization of a large department containing more than one hundred employees and several hundred different permissions represented by binary values, for instance, can hardly be interpreted by a human.



(a) Table visualization (b) Graph (c) SOM

Fig. 2. Different visualization types

Graph-based Visualizations. The usage of graph-based visualization techniques (Figure 2b) consisting of nodes and edges for presenting role structures has already been proposed by several authors (e.g. in [15]). Graphs can be used to browse data on different aggregation levels and provide cluster visualizations in order to highlight outliers or potential roles, resulting in a high perceptibility. Nevertheless, graph-based visualizations have major drawbacks in scalability. Kreuseler et al. state that they only scale until approximately 100 nodes [16], while access data of large organizations commonly exceeds this level significantly. Thus, even though graph-based visualizations are capable of displaying aggregated role information, they struggle with displaying large amounts of non-aggregated access data.

Neural Networks. SOMs (Figure 2c) have already been applied for outlier detection during role mining and data quality management [17]. Due to their high scalability and perceptibility, they are able to aggregate large amounts of data on the basis of a two-dimensional visualization. However, SOMs only allow for an aggregated data representation and can only be applied for displaying large amounts of data. If the amount of data is too low, the cluster quality significantly is reduced as SOMs position elements (like employees and their entitlements) in relation to other, potentially un-similar elements. If the basic population of displayed elements is too low or their similarity is too high, SOMs, for instance, display very similar elements within different parts of a network even though they should be located right next to each other. Practical experience shows that SOMs struggle when displaying access data consisting of less than approximately 100 employees.

Grid-based Visualizations. Similar to basic table visualizations, grid-based visualizations (Figure 3) are building on a two-dimensional matrix. Commonly, one axis is used for displaying employees while the other highlights their permissions. Figure 3 shows an example of an unsorted grid. Each grey colored cell represents a permission assignment while each empty cell shows that there is no such assignment. Previous work like [11-12] builds on a two-dimensional matrix in order to support the task of creating single roles. It, however, does not consider nor evaluate the usage of the grid consistently during pre- and post-processing steps of role modeling projects.

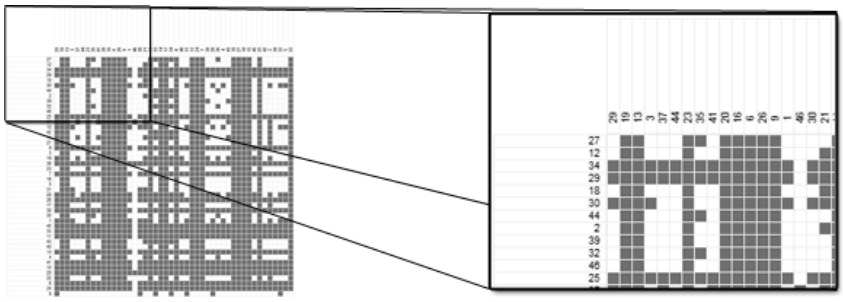


Fig. 3. Example of an access grid

In comparison to table visualizations, grid-based visualizations provide an easily interpretable overview of aggregated as well as non-aggregated data. By using colored symbols instead of characters, a role developer gets an improved overview of the underlying data structures, leading to a high perceptibility. Due to the two-dimensional representation of employees and permissions, grid-based visualizations offer a high level of consistency. In contrast to all aforementioned techniques, they can be applied during the pre-processing, role detection as well as post-processing activities of the RMPM. This high level of consistency gives the human interactor the option to work with the same visualization technique during all of his tasks. Due to these reasons we propose the usage of an enhanced grid-based visualization during the RMPM.

3.2 Characteristics of the Access Grid

In the following we shortly present the core characteristics of our proposed grid-based visualization (from hereinafter called access grid) before we embed it into the single RMPM activities in Section 4. In general, the access grid enhances the basic grid visualization technique by integrating intelligent **data sorting mechanisms** as well as a **high level of interactivity** and the inclusion of **business semantics**. It is thus no longer used as a trivial representation of two-dimensional data but rather acts as core element for information interpretation and human decision making during the RMPM.

Business Semantics. The semantic enrichment of data is one critical success factor during the application of the RMPM [7]. In contrast to two-dimensional matrix representations of access data, the access grid thus provides element coloring in order to display business-related information like employees' job title or department. The human interactor can, for instance, highlight departmental assignments of employees or visualize the homogeneity of employees' clustered job positions. This information supports him during the identification of over-authorized employees or the selection of one or more business roles from a large list of role candidates generated by role mining.

Intelligent Grid Sorting. As mentioned in [11] and [18], sorting of rows and columns is also critical when applying grid-based visualization techniques. Using a suitable sorting mechanism, interesting employee clusters and outliers might be visualized appropriately while the same patterns cannot be identified using another sorting mechanism. Therefore, the sorting of rows and columns is an optimization problem which cannot be solved in the context of identity management [11]. In general, there is a need for improved and sophisticated sorting methods which are able to focus on different aspects of used input data and reveal patterns and outliers depending on the current RMPM activity. Existing sorting mechanisms only facilitate simple similarity-based or graph-based algorithms based on pre-calculated roles.

Interactivity. Another characteristic and major improvement of the access grid is its interactivity. By not just statically visualizing data but rather allowing for human interaction and dynamic adaption, it increases applicability and simplifies the RMPM activities. The functionalities include common and practical features like drill-down and drill-up, panning and selecting. With zooming, it is possible to focus on details of the access grid or get an overview of the whole data. This is required as access grids commonly might spread over 100+ employees and 100+ permissions, leading to 10000+ cell matrices.

One main improvement of the access grid in comparison to existing visualization techniques is the deep integration into the RMPM by offering dynamic context menus. This, for instance, allows the human interactor to select certain areas of the grid and define underlying permission assignments e.g. as over-authorizations which need to be reviewed by a responsible authority like the head of the respective department. The grid offers the functionality required for delegating and forwarding the approval request to the appropriate business expert. The same holds for the role modeling task. Role candidates identified by a clustering algorithm can easily be highlighted, altered and saved for further approval.

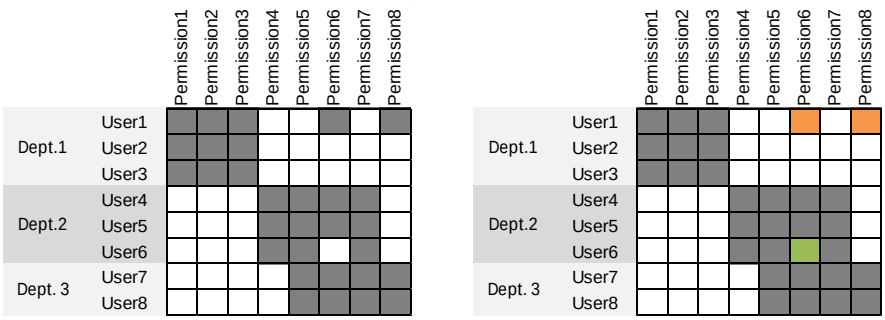
4 Embedding the Access Grid into the Role Mining Process

In this section of the paper we present the integration of the access grid into the RMPM following the concept of visual data mining [19]. The first goal is the improvement of the interpretability of automatically generated results by a human role developer. The second goal is the process-oriented manual generation of new knowledge by the role developer (e.g. the manual detection of outliers and roles) on the basis of an intuitive visualization of large amounts of data.

4.1 Pre-processing with the Access Grid

The first activity according to the RMPM is the pre-processing of input data. Companies starting a role modeling project commonly need to initially investigate their access privilege structures for errors like over-privileged employees or unsuited input data [7]. The access grid supports both, data cleansing as well as data selection.

By visualizing grouped access privileges, it allows for manually detecting outliers in the given data structures. The human interactor can drill down into departments of a company and analyze the respective access grids for conspicuous privilege assignments. Furthermore, automatically identified potential data errors can be displayed and highlighted. This way, the outcome of automated outlier detection mechanisms as well as role engineering input (like the enforcement of security policies defining rules for privilege assignments) can be validated. In addition, the exclusion of unsuited input data from further activities is supported by the access grid. In contrast to basic data filtering, e.g. using database queries, the displaying of business semantics (e.g. department assignments, permission criticality levels, etc.) allows for a simplified data selection. The role developer can, e.g., exclude unsuited data like critical entitlements that shall not be modeled into roles. The simplified example in Figure 4 underlines the suitability of the access grid for data cleansing and data selection activities.



(a) Access grid without highlighting (b) Access grid with highlighted outliers

Fig. 4. Using the access grid during pre-processing

In both sub-figures similar users suitable for role modeling can be detected (e.g. User 7 and User 8 sharing identical permissions) without additional business-related knowledge. It is also possible to identify users with untypical access privileges. Inspecting Figure 4a, the role developer could highlight the potentially excessive Permissions 6 and 8 of User1 and the missing Permission 6 of User 6. In the example in Figure 4b, automatic outlier detection mechanisms already identified and highlighted those privilege assignments as suspicious. The role developer then is able to decide whether to revoke or respectively grant the access privileges or mark them as valid exceptions.

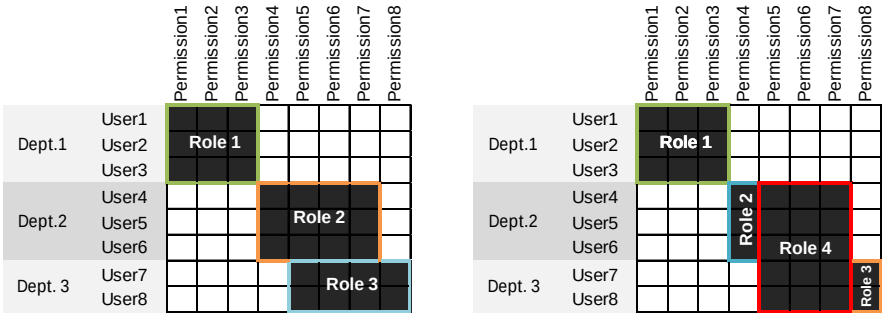
By displaying further attributes like the employees' departmental assignment or job title, cleansing and data selecting might benefit even when there is no feedback from business representatives available. This is a common challenge at the beginning of role modeling projects when companies start with a small team of IT-related role developers. The access grid allows for an initial interpretation of the access privilege quality. In case the structures reveal large areas of similar users, role modeling complexity is lower and the data quality is higher than in heterogeneous environments.

4.2 Role Detection Using the Access Grid

According to the RMPM, after pre-processing the actual role detection takes place. The access grid supports this task by allowing for interactive manual role detection on the one hand, as well as the validation of automatically generated or pre-existing roles on the other hand. This might even include pre-defined employee groups provided by business experts during role engineering activities. They can be displayed, essentially supporting the hybrid role development process.

The access grid furthermore supports various data sorting mechanisms. In case no roles have been pre-generated, it facilitates a similarity-based user sorting algorithm starting with the detection of user groups depending on the assigned access privileges. Subsequently, similar user groups and group members are clustered[2]. Permissions assigned to similar users thereby form a role candidate which can be easily detected by concentrating on columns in the access grid where all cells are filled. Another option is to sort users by their job description and permissions by their occurrence. This might reveal entitlements related to a single job or tasks in the organization and therefore lead to the identification of according roles.

While the above description uses the humans' ability to detect patterns in the access grid, another option is to iteratively run automated role mining algorithms and display the results after each run as shown in Figure 5. This might be useful in case a company wants to build their efforts on several different role detection algorithms in parallel, each with different parameters. A company might for instance use two algorithms, one detecting only flat roles (Figure 5a) and another one to detect role hierarchies (Figure 5b). In Figure 5b, Role 4 is a parent role of Role 2 and Role 3 using a top-down inheritance relationship. Displaying the respective results using the access grid, the identification and selection of the best fitting role set depending on the companies' goals can be simplified by a visual comparison. Moreover, the access grid might highlight roles covered by all algorithms as potentially good roles.



(a) Role configuration 1 (b) Role configuration 2

Fig. 5. Using the access grid during role detection

[2] Note that it is not the goal of this paper to present sorting mechanisms for the access grid. We have developed two sorting mechanisms; however, due to space constraints it is not possible to present them in detail. We plan to publish them in future work.

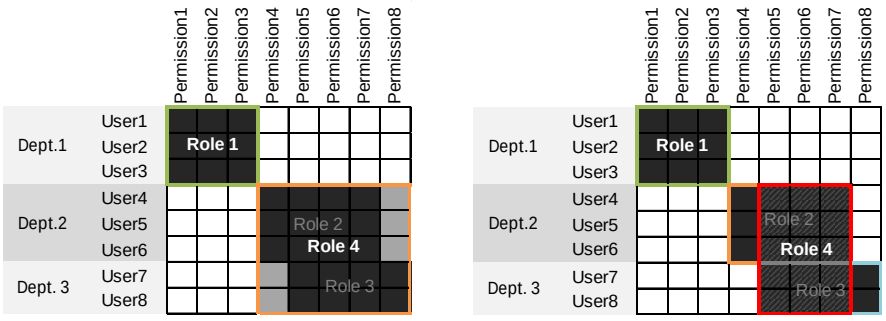
4.3 Post-processing with the Access Grid

During post-processing, the output data of role mining activities needs to be refined. This includes the optimization of role hierarchies, the splitting or merging of roles, as well as the further integration of business semantics to improve roles.

Hierarchy optimization can be supported by displaying overlapping roles in the access grid. The human interactor can select the overlapping area and model a role hierarchy. This refinement process can also be partly automated using a hierarchy modeling algorithm for detecting roles to be refined. This reduces the efforts of manual review by allowing for a visual inspection during role optimization. Without using the access grid, it is hardly possible to model and review role hierarchies within a large project setting consisting of thousands of employees and permissions.

The identification of roles spreading over various departments within a company is one challenge existing role modeling approaches struggle with. The access grid supports the integration of business semantics in order to support this task of role improvement. Even though the role developer analyzes one specific department, the access grid can, for instance, inform him about similar roles existing within other departments. The role developer can then refine those roles and their scope. He might aim at reducing administrative efforts and thus merge similar roles from various departments into one global role.

One example for role improvement is shown in Figure 6a where a role developer requests the merging of two existing roles (Role 2 and Role 3) into a new, larger role Role 4. In case the newly required access privileges (previously white areas in the access grid now covered by Role 4) are approved by a responsible authority, the merging can be executed. Additionally, business-related feedback resulting from a RMPM iteration can be used to improve role quality. In case a departmental manager alters a previously created role during his approval activity, he might request a role merging and a reduction of the permissions included in the role. In Figure 6b, for example, the role developer receives such a request, investigates the reasonableness of the decision and executes the merging of Role 2 and Role 3 into Role 4, essentially leading to an exclusion of certain permissions from the role definition (Permission 4 and Permission 8)



(a) Role with additional assignments (b) Possible hierarchy optimization

Fig. 6. Using the access grid during post-processing

5 Managing Insider Misuse Risks: A Case Study

After the application of the access grid during the RMPM has been presented, the paper continues with an evaluation of the proposed approach in a real-world application scenario, using a large, complex, and potentially erroneous dataset. We implemented the proposed access grid functionality as a web-based java application which is part of a larger tool[3] for analyzing identity data and business roles. The used dataset for this evaluation has been anonymized and originates from the IAM repository (Microsoft Active Directory) of a medium-sized organization in the retail sector. The company operates in large parts of Europe and has more than 3000 employees and nearly 1000 managed access privileges (Active Directory security groups). For readability reasons we present the results of the "Service" department consisting of 15 employees, 51 different access privileges and three sub-departments. Figure 7 displays the department's initial sorted access configuration showing the employees colored according to their departmental assignment on the left side. The anonymized permissions are represented by the columns. Grey Coloring of a grid element represents an existing access privilege of a certain employee.

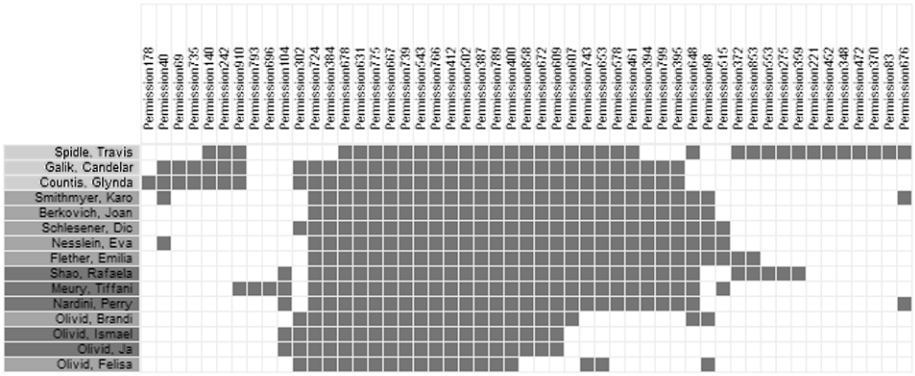


Fig. 7. Initial access grid of the "Service" department

Pre-processing. At first we applied the access grid during the pre-processing of the initial input data. During these activities, the access grid supports the role developer with its automated access privilege sorting and the inclusion of semantic information. We executed several automated data analysis algorithms to detect potentially erroneous privilege assignments and to subsequently highlight those outliers. Additionally, several over-authorizations in the predominantly white areas or on the edges of the bigger tiles in the access grid have been manually marked as outliers (Figure 8a, dark grey coloring). Subsequently, the responsible manager of the "Service" department has been asked to review the outliers in a hybrid fashion, resulting in an improved (and re-sorted) access grid (Figure 8b). Note that, depending on the company's preferences, the role developer himself might also be accredited to approve the outliers.

[3] http://www.nexis-secure.de

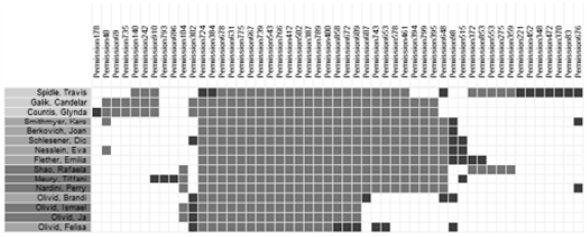


Fig. 8 (a). Data cleansing using the access grid - highlighted outliers

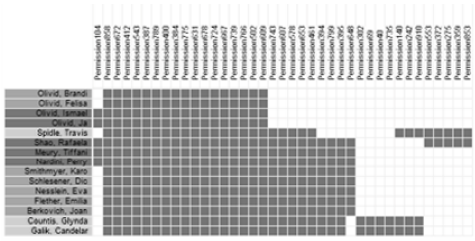


Fig. 8 (b). Data cleansing using the access grid - cleansed access data

Role Detection. After the input data has been cleansed, we used automated role mining algorithms to detect potential roles. Figure 9a displays the resulting three roles (grey, light grey and dark grey rectangles) representing the entitlements all employees share in the respective sub-departments. The role developer at this point is able to alter the role candidates by adding or removing access privileges or employees, essentially increasing or reducing the size of the rectangle representing the roles. He furthermore is capable of discarding identified roles or manually adding new roles. Figure 9b, for instance, shows the re-sorted access grid including one additional manually created role (dark grey rectangle). After the four defined roles have been approved by the responsible authority, the role developer might conclude role modeling for the "Service" department or add additional roles for the remaining uncovered access privileges (Figure 9b, grey coloring, at the right side). Practical experience revealed that using different sorting algorithms leads to altered role candidates. In future work we are thus going to investigate the effects of grid sorting on the manual role modeling in detail.

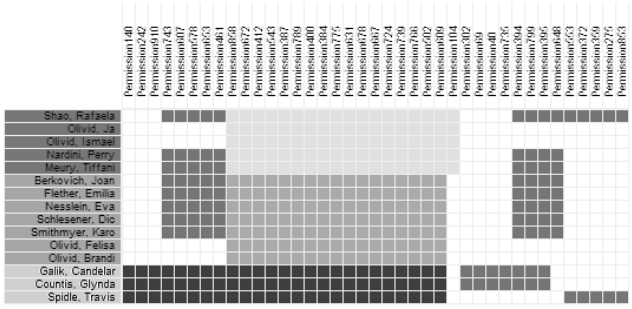


Fig. 9 (a). Role detection and creation using the access grid - automatically detected roles

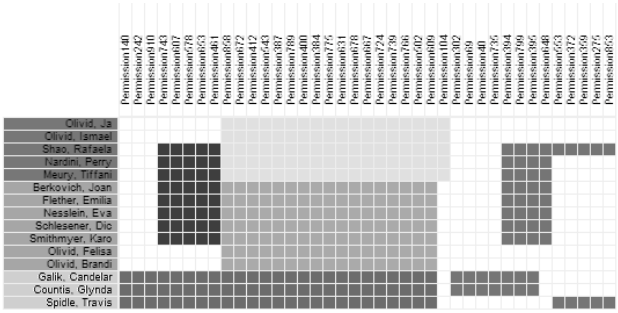


Fig. 9 (b). Role detection and creation using the access grid - manual role creations

Post-processing. Finally, the approved roles were post-processed and refined by setting up a role hierarchy. As mentioned, the three roles previously identified by the role mining algorithm represent the entitlements shared by all employees in the sub-departments of the “Service” department. The grid reveals a large overlap regarding their access privileges (see Figure 10a, light grey coloring). The role developer is thus capable of selecting the respective area and creating a new parent role for the three child roles, essentially setting up a role hierarchy.

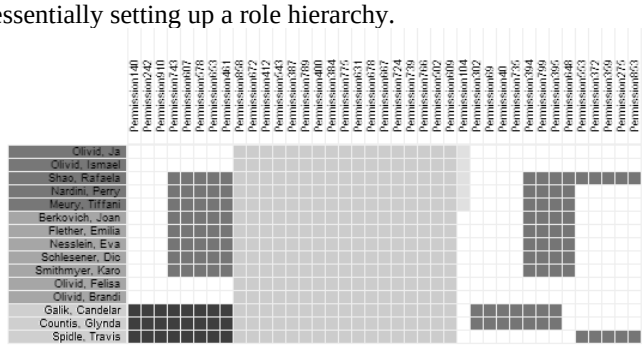


Fig. 10 (a). Role improvement using the access grid - hierarchy refinement

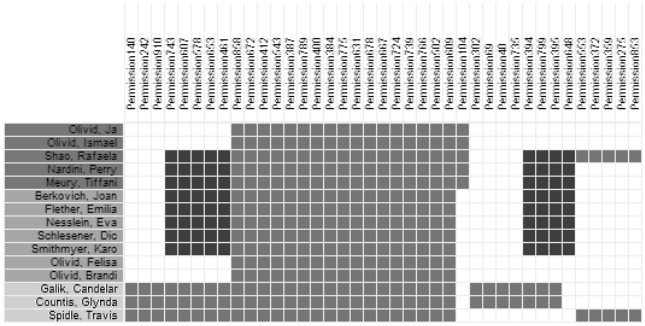


Fig. 10 (b). Role improvement using the access grid - single role refinement

Besides the role hierarchy modeling, other previously defined roles can further be improved. During post-processing, the access grid for instance highlights the potential extension of the manually defined fourth role (Figure 10b, dark grey coloring at the right side). In this case, the role developer previously missed to include those permissions within the role. During post-processing, he can facilitate the role extension suggested by the access grid and refine the role.

6 Conclusions

This paper proposed the usage of the so called access grid as an interactive visualization technique integrated into the Role-Mining Process Model for reducing insider misuse and supporting role modeling. The comparison of visualization techniques applicable during data cleansing and role mining activities in general in Section 3 revealed the access grid as the superior approach. Its high degree of usability in different project scenarios ranging from medium-sized to large-scale projects outpaces traditional limited visualization techniques.

During RMPM activities, the access grid provides intuitive decision support for responsible human interactors. Firstly, it has been shown that supporting the cleansing of excessive access privileges with the access grid leads to an improved user management within organizations. Potential insider misuse can be prevented by ensuring compliance with the principle of the Least Privilege. Secondly, the business semantic inclusion and interactivity of the access grid have been revealed as means to improve role detection and role refinement.

We have subsequently evaluated the benefits of the access grid throughout a real-world industry project. This evaluation, amongst others, revealed the impact and practical usability of the access grid and pointed at several potential future extensions. Above all, applying optimized grid sorting techniques as well as examining their effect on the access grid needs to be investigated during future research efforts as they have significant impact on data cleansing and role modeling. To further improve the human perceptibility, colorizing needs to be enhanced in order to allow for flexible and dynamic colorizing of different attributes. For applying the access grid in large environments with 10,000+ employees and permissions, approaches for data partitioning, e.g. based on departments, job descriptions or functional units in the organization additionally need to be investigated in detail, potentially including evaluation results from various case studies.

Acknowledgement

The research leading to these results was supported by “Regionale Wettbewerbsfähigkeit und Beschäftigung”, Bayern, 2007-2013 (EFRE) as part of the SECBIT project (http://www.secbit.de).

References

1. Corporate Trust - Business Risk & Crisis Management GmbH: Studie: Industriespionage 2012
2. Cleven, A., Winter, R.: Regulatory Compliance in Information Systems Research - Literature Analysis and Research Agenda. In: Enterprise, Business-Process and Information Systems Modeling. LNBIP, Vol. 29, pp. 174–186. Springer, Berlin Heidelberg (2009)
3. Sarbanes-Oxley Act of 2002, http://www.gpo.gov/fdsys/pkg/BILLS-107hr3763enr/pdf/BILLS-107hr3763enr.pdf
4. Basel III: A global regulatory framework for more resilient banks and banking systems, http://www.bis.org/publ/bcbs189.pdf.
5. Sandhu, R., Ferraiolo, D., Kuhn, R.: The NIST model for role-based access control. In: Proceedings of the fifth ACM workshop on Role-based access control - RBAC'00, pp. 47–63. ACM Press, New York (2000)
6. Gallaher, M.P., O'Connor, A.C., Kropp, B.: The Economic Impact of Role-Based Access Control. RTI (2002)
7. Fuchs, L., Meier, S.: The Role Mining Process Model - Underlining the Need for a Comprehensive Research Perspective. In: ARES 2011, pp. 35-42. IEEE (2011)
8. Probst, C.W., Hunker, J., Gollmann, D., Bishop, M.: Aspects of Insider Threats. In: Insider Threats in Cyber Security. Springer (2010)
9. Fuchs, L., Pernul, G.: HyDRo – Hybrid Development of Roles. In: Information Systems Security. LNCS, Vol. 5352, pp. 287–302. Springer (2008)
10. Neumann, G., Strembeck, M.: A scenario-driven role engineering process for functional RBAC roles. In: Proceedings of the seventh ACM symposium on Access control models and technologies - SACMAT'02, pp. 33–42 (2002)
11. Colantonio, A., Di Pietro, R., Ocello, A.: Role Mining in Business: Taming Role-Based Access Control Administration. World Scientific Publishing Co. Pte. Ltd. (2012)
12. Zhang, D., Ramamohanarao, K., Versteeg, S., Zhang, R.: RoleVAT: Visual Assessment of Practical Need for Role Based Access Control. In: 2009 Annual Computer Security Applications Conference, pp. 13–22. IEEE (2009)
13. Hoffman, P.E., Grinstein, G.G.: A Survey of Visualizations for High-Dimensional Data Mining. Information Visualization in Data Mining and Knowledge Discovery. Morgan Kaufmann Publishers Inc. (2002)
14. Lee, M.D., Reilly, R.E., Butavicius, M.E.: An Empirical Evaluation of Chernoff Faces, Star Glyphs, and Spatial Visualizations for Binary Data. In: Proceedings of the Asia-Pacific symposium on Information visualisation, pp. 1–10 (2003)
15. Zhang, D., Ramamohanarao, K., Ebringer, T.: Role Engineering using Graph Optimisation. In: Proceedings of the 12. ACM symposium on Access control models and technologies, pp. 139–144. ACM (2007)
16. Kreuseler, M., Schumann, H.: A Flexible Approach for Visual Data Mining. IEEE Transactions on Visualization and Computer Graphics 8, 39–51 (2002)
17. Fuchs, L., Pernul, G.: Reducing the Risk of Insider Misuse by Revising Identity Management and User Account Data. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 1 (1), 14–28 (2010)
18. Ong, K.-H., Ong, K.-L., Ng, W.-K., Lim, E.-P.: CrystalClear: Active Visualization of Association Rules. In: ICDM'02 International Workshop on Active Mining (2002)
19. Ankerst, M.: Visual Data Mining. dissertation.de (2001)