A Novel Heuristic Algorithm for Visualizing User Roles

C.Ranjith Kumar
Dept of CSE/Sasurie College of Engineering
Vijayamangalam,
Tamilnadu,
India

S.Selva Brinda
Dept of CSE/Sasurie College of Engineering
Vijayamangalam,
Tamilnadu,
India

ABSTRACT

In today's world commercial security and unique management products is highly adopted to role based access control (RBAC). Currently visualizing the user roles instead of raw data will make a significant impact in business trends. Earlier process used many heuristic algorithms with which visual role mining was achieved whereas the amount of noise within the data and correlation among roles made it is limited. To overcome the drawbacks of the above technique we proposed two algorithms: ZOOMING & DATA FILTERING. The later proposed a technique is used for the issue of reducing the noise among the data. Secondly, a novel algorithm is framed for visualizing a single user in multiple domain roles. Results will be demonstrated by using real time data.

General Terms

Access controls, data and knowledge visualization, mining methods and algorithms.

Keywords

Data Mining, Role Mining, Role Based Access Control, Multi domains.

1. INTRODUCTION

With continuous growth in the number of information objects and the users that can access these objects, ensuring that access is compliant with company policies has become a big challenge. Role-based Access Control (RBAC) a policy neutral access control model that serves as a bridge between academia and industry - is probably the most suitable security model for commercial applications. Among all proposed models, Role-Based Access Control (RBAC) has become the norm in most organizations. This success is greatly due to its simplicity: a role identifies a set of permissions; users, in turn, are assigned to roles based on their responsibilities.

Recently, there has been an increasing interest in using automated role engineering techniques. All of them seek to identify the fact of roles embedded existing access permissions.

Since these approaches usually resort to data mining techniques, the term role mining is often used as a synonym.

2. RBAC MODEL FOR SINGLE DOMAIN

Single domain analysis is elaborated by using the following model shown in the Figure 1.

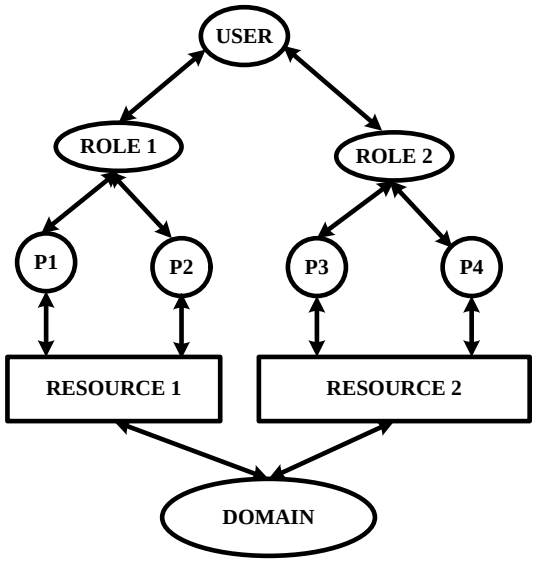

Fig 1: Single domain architecture

In this model, an autonomous agent or a human being is considered as user, a collection of privileges to perform a certain task is defined as role, a privilege is an access mode that can be exercised on objects.

A user can be assigned to a number of different roles, and a role can have multiple users. A role may have multiple permissions (P1, P2, P3, and P4) and the same permissions can be associated to different roles.

3. RBAC MODEL FOR MULTIPLE DOMAINS

Multiple authorities manage different security policies with various set of users and objects and it is wholly termed as multiple domain models. An architectural model for multi domain users is shown in figure 2.
Here the users can access the objects even outside their environment. On the other hand, with the development of the

Internet and e-business, there are many requirements that users in a secure domain would like to share objects with users in other secure domains.

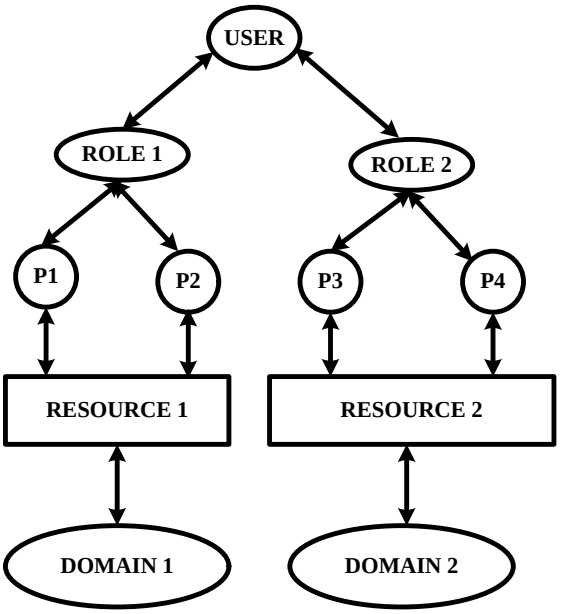

Fig 2: Multiple domain architecture

Based on trust credentials, the permissions of a single secure domain are divided into three groups:

1) Permissions that can be accessed by other domain users without the constraints of trust credentials

2) Permissions that cannot be access by other domain users.

3) Permissions that can be accessed by other domain users under different constraints of trust credentials.

4. TOOLS ENROLLED FOR RBAC MANAGEMENT

The role mining objective is to analyze access control data in order to elicit a set of meaningful roles that simplify RBAC management.

To this aim, various business information can be analyzed but user-permission assignments are the minimal data set required. A natural representation for this information is the binary matrix, where rows and columns correspond to users and permissions, and each cell is "on" when a certain user has a certain permission granted.

Table (a) Input data

Table (b) Associate Candidate Roles

Role	Permissions	User	Domain
R_1	{ p_1, p_3, p_4}	u_0	d_1
R_2	{ p_1, p_2}	u_1, u_2	d_1, d_2
R_3	{ p_2, p_4}	u_3	d_2
R_4	{ p_1, p_2, p_3}	u_4	d_1, d_2
R_5	{ p_3, p_4}	u_5	d_1

Table (a) shows a possible set of user permission & domain assignments. The figure 3 is definitely an associative.

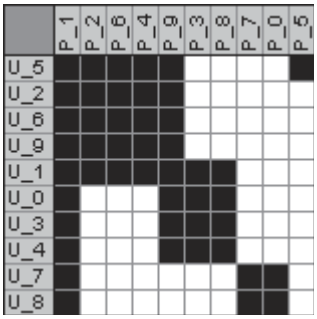

Fig 3: Sorted Matrix

Here p_1 may be assigned to roles R_2;R_3;R_4, thus making R_1 no longer necessary. Alternatively, if p_1 represents a permission that should always be granted to all users, keeping R_1 may be more advantageous.

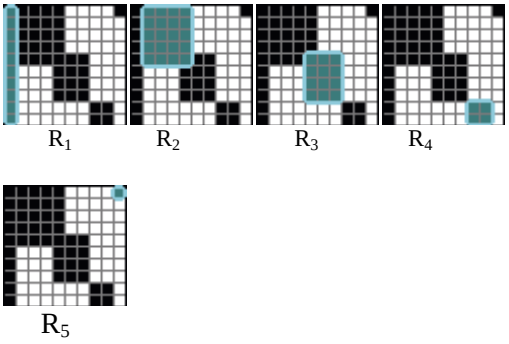

Fig 4: Visual representation of roles.

The user u_5 is the only one that has permission p_5 granted. This finding warns about a potentially wrong assignment due to causes such as privilege accumulation or illicit authorization.

5. VISUALIZING MULTIPLE DOMAIN ROLE

Multiple domains user permission assignment			
{u_0,p_1,d_1}	{u_0,p_3,d_1}	{u_0,p_4,d_1}	{u_1,p_1,d_1}
{u_1,p_2,d_1}	{u_1,p_1,d_2}	{u_1,p_2,d_2}	{u_2,p_1,d_1}
{u_2,p_2,d_1}	{u_2,p_1,d_2}	{u_2,p_2,d_2}	{u_3,p_2,d_2}
{u_3,p_4,d_2}	{u_4,p_1,d_1}	{u_4,p_2,d_1}	{u_4,p_3,d_1}
{u_4,p_1,d_2}	{u_4,p_2,d_2}	{u_4,p_3,d_2}	{u_5,p_3,d_1}
{u_5,p_4,d_1}	{u_5,p_1,d_2}	{u_5,p_2,d_2}	

Now describe a viable, fast heuristic algorithm called zooming & data filtering. Given a set of roles, this algorithm is able to provide a compact representation of them. In particular, it reorders rows and columns of the user-permission matrix to minimize the fragmentation of each role. Despite being relatively simple, it provides a good though not necessarily optimal and fast solution to the otherwise intractable OMP problem. In particular, its running time is $\varphi\left(n\times\left(|roles|+\log n\right)\right)$ where $n=\max\left\{|Users|,|Perms|,|Domains|\right\}$. Also for visualizing a single user in multiple domain roles is to be implemented.

5.1 Role validation algorithm

Algorithm: Role Validation Algorithm
(Applied role R, User X, Domain D)
Input:
X: identification of the user. Applied role R: the role that user applies for V.
V: the role set including role R and its parent roles in the role hierarchy.
Q: a FIFO queue.
Mark []: indicator of a visited/unvisited role.
Di-Parent [r]: direct parent role of role r.
D: Denote Different Domains
Output:
Authorized role R to the user or refuse message.

```
{
For each u ∈ V − {R}
Mark[u] = 0;
Mark[R] = 1;
Q ← {R};
While Q <> 0 do
{
Remove R from Q;
If X ∈ the authorized user set of role R And D ∈ the authorized domain set of role R {
Output R;
}
For each v ∈ Di-Parent[R]
{
If mark[v]=0
put v on Q ;
}
}
Output refuse message
}
```

Analysis of the algorithm:

For the applied role R, each direct or indirect parent role of R, S, is places in the queue once, assume the number of S is L, the computation complexity of the algorithm will be O(L).

5.2 Multiple domain access algorithm

Input:
Applied other domain privilege M: the required other domain privilege M.
Authentication credentials of the other domain user H: the authentication credentials the other domain user provided.

Output:
Authorized foreign role R to H or refuse message.

```
{
For each foreign role R of the foreign privilege M
{
if authentication credentials of R ⊆ H {
other domain role R is authorized;
output for other domain role R;
}
}
output refuse message;
}
```

5.3 ADVISER algorithm

Fast heuristic algorithm called ADVISER (Access Data VISualizER). Given a set of roles, this algorithm is able to provide a compact representation of them. In particular, it reorders rows and columns of the user-permission matrix to minimize the fragmentation of each role. Despite being relatively simple,

```
ADVISER(USERS,PERMS,ROLES,DOMAINS,UA,PA)
{
U ← SORTSET(USERS,UA,ROLES,DOMAIN)
P ← SORTSET(PERMS,PA,ROLES,DOMAIN)
RETURN U,P
}

SORTSET(ITEMS,IA,ROLES,DOMAINS)
{
```

$\overline{ITEMS} \leftarrow \{I \subseteq ITEMS \mid \forall i,i' \in I, roles(i) = roles(i'), domain(i) = domain(i')\}$

For all I ∈ $\overline{ITEMS}$ sorted by descending areas of domains (I) do
{
For all I ∈ $\overline{ITEMS}$ sorted by descending areas of roles (I) do
{
Sort Maximum Proceeding to minimum
}
}
Return SortSet of Items
}

Adviser Algorithm Description:

ADVISER is based on some intuitions, summarized in the following:

1) Introducing a "gap" in the visualization of "large" roles (namely, those roles that involve many users and permissions) increases more than introducing gaps on smaller roles. Hence, larger roles should be better represented.
2) The more fragments in the visualization of a role, the higher the role visualization cost.
3) Reordering users but not permissions only affects the number of gaps between columns, and so do permissions.

6. PROBLEM FORMULATION

In this, formalize the problem, offering a tool for the identification of the best representation for a given set of roles. To this aim, first summarize some concepts of the RBAC model. For the sake of simplicity, role
hierarchies and constraints are not considered. Entities of interest are

1) PERMS, USERS, ROLES, and DOMAIN all access permissions, users, roles, and domain respectively.
2) UA $\subseteq$ USERS X ROLES X DOMAIN, all role-user domain relations.
3) ass users : $\text{ROLES} \to 2^{\text{USERS}}$,the membership function for users, that is $ass\_users(r) = (u \in USERS \mid \langle u, r, d \rangle \in UA)$
4) PA $\subseteq$ PERMS X ROLES X DOMAIN, all role-permission relations.
5) ass perms : $\text{ROLES} \to 2^{\text{PERMS}}$, the membership function for permission, that is $ass\_perms(r) = (p \in PERMS \mid \langle p, r, d \rangle \in PA)$

6.1 Advantage of proposed system

Zooming algorithm is based on a noise removal algorithm. A fourth-order PDE is introduced to image denoising, which is to recover an image from a noisy observation.
The data filtering algorithm have the ability to remove the error so that they cannot be detected, by manual inspection, after the respective dataset has been processed.
The evaluation method called cross validation is probably the most important and wide ranging method, since it is able to compare the performance of any models or filters to each other and also optimize the performance of any model or filter in a straight forward fashion.
Finally a novel heuristic algorithm will be developed for single user in multiple domain roles.

7. CONCLUSION

Several contributions have been provided. First, offered a formal description of the visual role mining problem. Secondly it was demonstrated that constructing the binary matrix representation of user-permission relations in multiple domains. An efficient, tunable, and probabilistic tool referred to as EXTRACT and Foreign Role Authorization Algorithm has been elaborated.
As for future work, solutions can be extended in several directions for making more fine visualization in case of huge data analysis.

8. REFERENCES

[1] Alessandro Colantonio, Roberto Di Pietro,Alberto Ocello, Nino Vincenzo Verde, "Visual Role Mining:A Picture Is Worth a Thousand Roles", IEEE *Transactions on knowledge and data engineering*, vol. 24, no. 6, june 2012

[2] S. De Capitani Di Vimercati, S. Foresti, P. Samarati, and S. Jajodia,"Access Control Policies and Languages," *Int'l J. Computational Science and Eng., vol. 3, no.* 2, pp. 94-102, 2007.

[3] J. Vaidya, V. Atluri, and J. Warner, "RoleMiner: Mining Roles Using Subset Enumeration," *Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06)*, pp. 144-153, 2006.

[4] I. Molloy, N. Li, T. Li, Z. Mao, Q. Wang, and J. Lobo, "Evaluating Role Mining Algorithms," *Proc. 14th ACM Symp. Access Control Models and Technologies (SACMAT '09)*, pp. 95-104, 2009.

[5] J. Vaidya, V. Atluri, and Q. Guo, "The Role Mining Problem: Finding a Minimal Descriptive Set of Roles," Proc. 12th ACM Symp. Access Control Models and Technologies (SACMAT '07), pp. 175-184, 2007.

[6] A. Colantonio, R. Di Pietro, A. Ocello, and N.V. Verde, "A Formal Framework to Elicit Roles with Business Meaning in RBAC Systems," Proc. 14th ACM Symp. Access Control Models and Technologies (SACMAT '09), pp. 85-94, 2009.

[7] M. Frank, D. Basin, and J.M. Buhmann, "A Class of Probabilistic Models for Role Engineering," *Proc. 15th ACM Conf. Computer and Comm. Security (CCS '08),* pp. 299-310, 2008.

[8] J. Vaidya, V. Atluri, and J. Warner, "RoleMiner: Mining Roles Using Subset Enumeration," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 144-153, 2006.

[9] M. Frank, A.P. Streich, D. Basin, and J.M. Buhmann, "A Probabilistic Approach to Hybrid Role Mining," *Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09),* pp. 101-111, 2009.

[10] A. Colantonio, R. Di Pietro, A. Ocello, and N.V. Verde, "Mining Business-Relevant RBAC States through Decomposition," *Proc. Security and Privacy-Silver Linings in the Cloud*, pp. 19-30, 2010.

[11] R. Gupta, G. Fang, B. Field, M. Steinbach, and V. Kumar, "Quantitative Evaluation of Approximate Frequent Pattern Mining Algorithms," *Proc. 14th ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '08)*, pp. 301-309, 2008.

[12] A. Colantonio, R. Di Pietro, and A. Ocello, "Leveraging Lattices to Improve Role Mining," *Proc. IFIP 23rd Int'l Information Security Conf.*, pp. 333-347, 2008.

[13] A. Colantonio, R. Di Pietro, A. Ocello, and N.V Verde, "A New Role Mining Framework to Elicit Business Roles and to Mitigate Enterprise Risk," *Decision Support Systems, vol. 50, no. 4, pp.* 715- 731, 2010.

[14] Cungang Yang, "An Object Oriented Role-based Access Control Model for Secure Domain Environments," International Journal of Network Security, Vol.4, No.1, pp.10–16, 2007.

[15] D.A. Keim, G. Andrienko, J.-D. Fekete, C. Go¨ rg, J. Kohlhammer, and G. Melanc¸on, "Visual Analytics: Definition, Process, and Challenges," Information Visualization: Human-Centered Issues and Perspectives, vol. 4950, pp. 154-175, 2008.

Ranjith Kumar C received his Master of Computer Application degree from Erode Arts College, Erode. Currently he is pursuing M.E in Computer Science and Engineering at Sasurie college of Engineering, Vijayamangalam, affiliated to Anna

Selva Brinda.S received her Master of Engineering degree from Annai Mathammal sheela Engineering College,Namakkal, Anna University. Received her Ph.D Mother Teresa Women's University,Kodaikanal