An Access Control List for Role-Based System: An Observation and Recommendation

Sharipah Setapa and Tengku Puteri Suhilah

***Abstract*—Access control list have been implemented in many area. This concept of rules can be used to manage user authorization in the large organization. It can be designed based on standard Role Based Access Control List (RBAC) or equivalent. Role access control list should be surrounding by module such as identification, authentication, authorization and auditing which can make the system effective. Role mining will help to define each task correctly in order to avoid conflict when the system establish. Once the identification is been provided system will authenticate based on active directory or through protected database based on hardware of software. A strong authentication and encrypted will increase user confident to access and employ role based system. The database can be located in the same system or it can be in different location. The structure of access control list and the relation with database will define the efficiency and performance of the system. Once the system is working an audit trail will be provided to check all processing and action. A good policy will defined the correct access to specific task. The management of role and policies will assist the access control list to perform as been intended to reduce potential risks and vulnerabilities by embed in the network or through VPN workflow. In this paper architecture, design and policy will be further discussed through the observation and recommendation to increase the maturity of access control in the organization.**

***Index Terms*—Access control list, flexibility, role, security, embedded.**

I. Introduction

Internet has been used as an intermediate gateway to transfer data and communicate. It became like a cloud in which information is available anytime and everybody can access it. Then come access control list to restrict the access. It helps by restrict the content, provide permission to the user and control the traffic flow. Access control list also can block communication between computers through hardware devices or software. This is needed because it can give a protection and level of confident to the owner of data and to organization. An access control list in traditional Unix system and window can be described as below in Fig. 1:

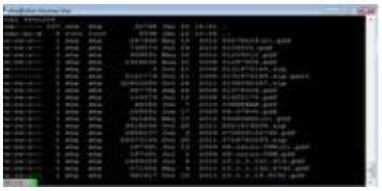

Fig. 1. Access control list.

In Unix environment when user login into the system, a role as a user or as system administrator is been created. Read, write and execute permission is been given to them. Any user is authorize to get access to the file when his or her name is been added. In window operating system the permission will be given by type the name of the person to access the file as shown in Fig. 2. Permission read and write will be tied to that name.

Fig. 2. Access control list in window.

Other function of access control list is to control the network traffic at the router interface. Router will be used to examine, block or forward the packet from be accessed. In traditional method, system and application permission will be managed by group. Application, permission and group member will be assigned by system administrator. System owner will give permission for the user to access the application. It acts like a channel which can protect your information from fall into the other party. When the organization is large an access control list will be difficult to maintain, implement and administer. Based on National Institute of Standards and Technology (NIST) an access control list which is Role Based Access Control (RBAC) will predominant model for advanced access control in large enterprise [1]. The traditional access control list and RBAC have one common goal which is to provide security.

II. Methodology

Different organization can have different role, action, resource hierarchy and operation. In order to define role correctly in the organization, an analysison how the organization operation, structure, resource hierarchy and multiple operation for one role have to be explored. Input from user and their experience need to be included because it was not capture in the manual operation. Role should be observed from business perspective and then bind with policies. These policies will explain about what task, resource list or application that can be authorized for the role. Access control will be mapped for each job function such as role and permission [2]. Role will change when user moving to another place, state or country but it still can perform the

Manuscript received September 13, 2013; revised January 10, 2014.

Sharipah Setapa is with MIMOS, Malaysia (e-mail: sharipah@mimos.my).

same operation with a bigger coverage.

User database information needs to be updated synchronously with access control list system in order to avoid conflict. If roles was defined partially this will be ineffective for the system and organization. Role mining will help to extract useful information of role based on resource. Without clear picture of roles and resource list a system that was built will missing certain criteria of organization.

III. Role Based Access Control

Role based were created to give access to authorize user only with a clear task and action. RBAC is flexible accesses to implement Discretionary access control (DAC) or Mandatory Access Control (MAC) which is traditional access control list. Integration, maintain and scale will be difficult without proper standard structure. Table I show the comparison between them [3]. Traditional access control list only assign to low level data. The assignment of permission and the reasoning in RBAC during the operation will make sure proper assignment of the resource can be given.

TABLE I: Comparison Between RBAC and Traditional ACL

	RBAC	Traditional ACL
1.	Group level permission	Personal permission
2.	Set by system owner	Set by data owner
3.	roles access	Based on data/ source
4.	Centrally administered	Administered on the resource
5.	Permission is static	Permission are often changed
6.	Reasoning	No Reasoning
7.	Useful for organization	None
8.	Assign permission to specific operation	Low level data object

Company with large employee is using role based to restrict the access. It is also known as role-based security. This role based can be summarized as shown in Fig. 3.

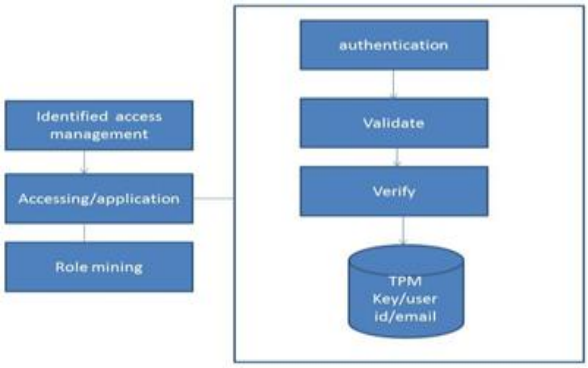

Fig. 3. Role based security.

Verification and validation will be based on information in database. It can be email address, employee ID and pre shared key. Other trusted key such TPM key which come together with TPM chip is encourage to be used. It is suggested to capture core measurement which is store in Platform Configuration Register (PCR) as a benchmark for integrity measurement. Core measurement can also be implemented without TPM, by storing the measurement in protected database. If the measurement is mismatch then the verification will be failed. All this information must bind with employee in order to make sure the verification and validation is success.

A basic step of the system based on RBAC can be described as below:

1) An authentication will be performed based on any token, credential or based employee information.
2) Once the authentication is successful then it will allowed to access the system.
3) Operation can performed if user is authorised for each resource based on policies which has been defined previously.

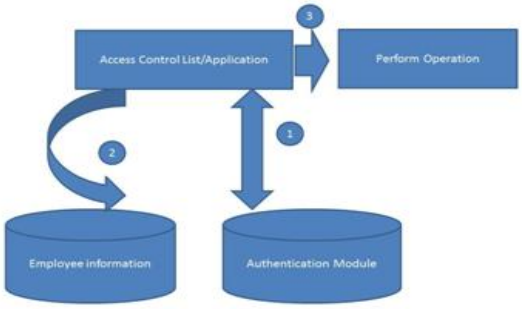

Fig. 4. Basic step.

Each employee has their role based on job function. In certain situation an employee can have more than one roles based on appointment from their superior. One ultimate user is needed to assign staff to become more than one role.There are three primary rules are defined for the role managementor RBAC [4]:

1) Role assignment
2) Role authorization
3) Permission authorization

In the role assignment, system admin will have the ultimate privileges to assign user with a role in the system. It can assign everybody to be any role. When role be assigned an authorization will be given to them. He/she can give a permission to approved or reject any subject under their authorization.

A set of permission with different facilities of privilege will be capable when different role is login into the system. There are a lot database which support RBAC such as Microsoft active directory, Microsoft SQL server, PostgreSQL and SAP. The alignment of data employee must be synchronized with the parameter in the application. If the information is missing or not updated in the database then the access control list will not listed specific user information. A performance or time to response is based on how database been allocated or arranged. This database performance can be influenced by other component in network infrastructure.

By administrative and manage privileges is the best practice through one single application because it reduce employee downtime, efficient access control policy administration. In the backend process, a communication between database and application need to be study. The employee role and data structure to migrate into the system need to be clear and align with the system and vice versa [5].Without that a conflict during authentication and authorization for each role will happen. Governing the data, downtime, ease to use, flexibility and scalability are major criteria to develop a better access control list.

Role portion can be designed through the different

database or the same database which have user information. If the database of user information can afford to adapt role and resource, then it can be implemented but it depends on the flexibility of the software, hardware and capacity of hard disk.

IV. Discussion

In order to protect from intruder for role based access system, it must have security feature which are [6]:

- Authentication services-to securely identify a user, which require the user's name and some form of proof
- Authentication with encryption-The ability to ensure that authenticated parties can communicate without interception, modification or spoofing
- Auditing-The ability to identify the source of security changes to the system, including access
- Security policies

The authentication happens in order to verify whether user is correct or not to access the system. This transmission is needed to provide verification from database. Unfortunately the transmission between authentications is not encrypted. User information can be sniff and view in clear text if not be encrypted.

Every time to access a system after been logout a same process will happen. A same password and username will be given unless users want to change frequently. A smart password which includes number, capital or small letter is encouraged. In this stage it is static, because it depends on user to change the password. This traditional authentication can be assumed as static and not dynamic. Other authentication such as Kerberos will give a ticket for accessing certain application or service. When receive a ticket user will represent a ticket to the application before be granted [7]. This method although look strong but it still can be sniff through technology hacking which been up to date as per today.

Using email to authenticate has a weakness. If the staff is changing the email without informs the management then the database is not updated. This will cause the access control to be failed. As a result someone can use the previous authentication to gain the access. Other question that needs to be figure out is how to manage multiple emails in the system. It is suggested that staffs that not belongs to the organization, his or her email should be deleted from the database as soon as possible.

Role mining will help to study one role which has multiple policies. Some other policy will be used by other role to access the resources. By merging certain policy to other role will give access to other role to do authorization. Duplication in role can be reduced through role mining. The new security module can be added under accessing/privileges. In real organization with large employee, each staff has more than one role. Role name and designation is to enforce the security policy.

In order to define and do analysis of the role in certain organization a discussion need to be done. It cannot be defined in a short time. System was built was not meet the expectation due of the resource list and role is not be captured properly. When analysis is been done for the role, an expert of the business organization need to be there together with the IT person to clarify it. This will help to convert the role into the System.

A. Weakness

In large organization there are users which can access the same resources with different role. When access control list be designed in the system, an authorization should not be conflict with the role. If different role can do the same authorization or permission, a filtering or expert rules need to be created.

Authorization only can verify through database which consist of information of user ID, email and password. If the users retire, their authentication can be used by other person or their colleague. An element or feature to disable and enable the authentication needs to be design if the user work again in same department after retired.

Role based is using as access control list based on the level of role. Once the role is changing then the level will not valid. In order to gain access the role, an authentication must be authenticated by using email, employee ID or password.

B. Optimization Access Control list

The role mining is important for us to understand how the role will behave. If the same role is also to assign to other staff then it need to define clearly. The same role can be solved through grouping. If the resource only to view, a role of group for view the same resource should be created. This problem will happen to large organization which has a role to view but not authorized to change, modified or approve.

C. Role-Based Ontology

Semantic technology can simplify access control list and provide interoperability between a comprehensive access control levels [8]. When the access control list is large, system administrator cannot handle and have a difficulty to manage and decide [9]. Useful information will help system administrator to decide and segregate each role and hierarch which needs to be taken. An automatic analysis is useful for system administrator who has difficulty to gain the information when the situation has multiple roles, different condition for different situation. A rule-based can be added in the system which gives the output for each suitable role for different function. There are certain criteria of policies and how certain policies can be allowed by multiple roles. A rule base is logic approaches which help system administrator to decide it.

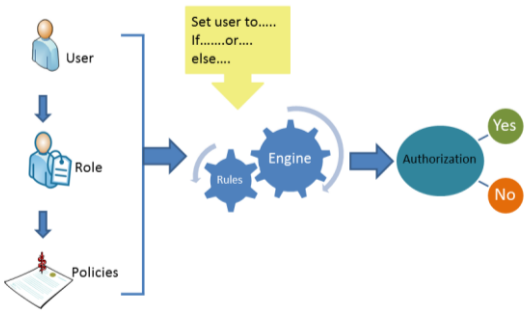

Fig. 5. Role based ontology.

Role base can be described in a basic scenario as shown in Fig. 5. User can be clerk or supervisor which have different role. A clerk can only purchase order but he/she cannot approve the same order at the same time. The supervisor who

acts as an approver will review and approve the purchase order. But in some circumstances, the clerk can also approve his/her order if the policies allow it but it should be based on some conditions that already defined in the rules engine.

D. Scalability and Flexibility

Role can be assigned statically by administrator and can cause a limitation. Several applications which been divided into sub child and combination of several policies to be accessed by particular group of role will make it complicated. Semantic technologies can provide relevant, useful information, interoperability of role, combination of policies, resource and application [10]. The system can be expand without changing the structure, which in this case can reduced the developer time to develop from scratch, if new module need to be developed.

In the access control list system administrator or user which have privileges will assign the policy which already be defined previously. This policy is located in another system. This is assumed that only eligible user can assign it. In another organization which need specific user to defined policy or task, a privilege need to be given to them.

E. Comparison Open Source and Commercial Product Scalability

In open source the product is difficult to learn compare to commercial product which been supported using Graphical User Interface. Like any other product from open source a community support is strong to increase the implementation [11].

TABLE II: COMPARISON OF OPEN SOURCE AND COMMERCIAL

Open source RBAC	Commercial product
Learning curve	Learning curve
Difficult to configure, command line	GUI
Started difficult	Easy to start
Community support	Unsatisfactory support

Role be group as domain in SELinux as shown in Fig. 6. Enforce be select as a target policy. Then role be grouping into domain. If domain A and domain B is fall under role C, however to go to domain B a rule need to be created for the transition from domain A to domain B. SELinux is one of the examples which used the concept of RBAC [8].

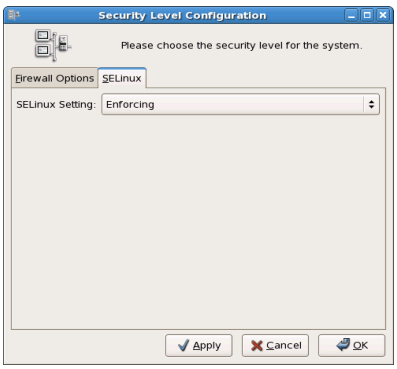

Fig. 6. Role be enforced through SELinux.

This RBAC is based on the application. Other RBAC for the device been called as kernel-RBAC model. It is one of the methods to protect the kernel under various operating systems [12]. This will increase a security for the embedded device.

In working life in organization, as a staff our role can be fall under system administrator, ordinary user or super admin. Staff with super admin can access full application whereas ordinary staff has limited application and resource access. This is based on rules or policy which tight with that application. Ontology come when the relation and mapping a role is not straight forward to be captured. These will a cause a difficulty to assign it by system administrator. Group, application and role are a standard role management. Every role management has this concept [8], but when this standard had been absorbed into organization, some modification or extra module can be added to suit the organization structure. Usually during our study the standard is not totally tally with the environment of the organization. Without this a system is like a normal standard access control list without organization behavior. The initial step to build the system is to get a firm requirement which been influenced by organization structure. Only with that the system can be fully utilized.

Role can be filter by all roles, single roles and multiple roles. Role 1 can be match with resource 1. But at the same time Role 2 also need a resource based on role 1. Filtering technique can be based on knowledge based expert system or rules to define the authorization. A Filtering technique can be knowledge based or rules to match suitable resource for each role. This can be useful if one roles need to access to other resources which by default belong to other role as shown in Fig. 7.

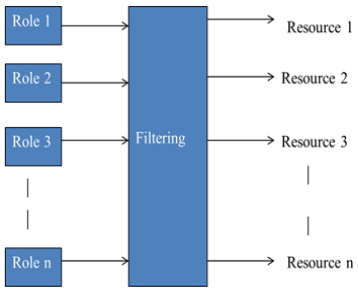

Fig. 7. Role 1, 2, 3 ..role *n* with respective resource.

V. RECOMMENDATION

Using email address, employee ID and password is one of the methods for accessing the system. The weakness is the application must have the identification store or embed in the application or database. The database which stores the identification is not encrypted. It is in clear text. If someone can gain access to the database and application all user information can be retrieved. People will try to guess the person email to access the system if it using the email as a token. When the authentication is success then authorization will take part. The resource will be based on the role which be authorized by the policy which be defined previously. The role is the one that control the authorization. When define the policy for each role a caution step will help to avoid mistake when define the resource for each role in large organization.

But to add more value and comprehensive an audit trail module can be added to support all the action. This can act as a history if previous action needs to be monitored. Policies can be based on rule, employee id and job function which can be used to create an access control list into the system.

Every action which is rarely be used but can give impact to

the organization or system, need to capture in audit trail. It can help to remind or help to do analysis what have been done. This will reduce the time to recall the previous action. With audit trail employee with specific role can recall the action User who become system administrator have found how useful audit trail to capture certain action for the purposes of troubleshooting.

Certain user has same job function and it can be put under one group. This will create a large group, and can cause a problem. Once the group is establish a role need to be defined. The role will differentiate each group and if the group meets the condition then the respective group will do the action. A mapping will map again each group. A detail condition in role will help to defined narrowly to respective group.

This is based on the group but how about policy for individual user which only he/she can do the role such as CEO (Chief Operating Officer). A role mining will help to define the role properly.

In large organization it is seldom to have one staff for one role only. Although staffs have one role it is possible the resource be accessed is more than one. If the role cannot be defined properly then it is better to avoid having one user for one role

Policy and role is based from business procedure. Once the role condition is fulfill then a policy need to check. If security policy is meet then the condition for the role will be fulfill. From there a security policy will be used to give access to the resources for the role. Role is the element to implement the authorization which relate with application and resources. To create security policy and security role, a system administrator needs to understand the relationship between role and how role can access the resource. A policy can have a few conditions depend on the organization.

Resource in the network which be gained through Virtual Private Network (VPN) is not been control by the tunnel which been established. VPN only capture the workflow only. This policy and role can be embedded into the VPN flow to protect the resource from unauthorized access. Although it look impossible, by embed the role and policy which be define previously, this will give two layer of security in VPN [13]-[15].

VI. Conclusion

Role and access control is important to protect from misuse of resource in the organization. A resource which been accessed from outside organization by using VPN should be embed with access control. By adding access control in the network will protect from virus or misuse of resource. This can be done by add another process in the workflow of the VPN network. The workload will be increase in order to design a system which using existing infrastructure. However to support it a research or literature need to be done further.

References

[1] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST Model for Role-based Access Control: Towards a Unfiied Standard," in *Proc. the fifth ACM workshop on Role-based access control 47-63*, 2000.

[2] S. Kim, D.-K. Kim, K.-J. Lu, S. Kim, and S. Park, "A feature-based approach for modeling role-based access control systems," *The Journal of Systems and Software*, vol. 84, issue 12, pp. 2035-2052, December 2011.

[3] *An Introduction to Role-Based Access Control*, ITL, NIST, December 1995.

[4] X.-S. Feng, B. Ge, Y. Sun, Z.-W. Wang, and D.-Q. Tang, "Enhancing Role Management in Role-Based Access Control," in *Proc. 3rd IEEE International Conference Broadband Network and Multimedia Technology (IC-BNMT)*, 26-28 October, 2010, pp. 677-683.

[5] P. Gietz and M. Widmer, "Pros and Cons for using LDAP as backend for an RBAC system (2011)," in *Proc. Third International Conference on LDAP (LDAPCon)*, Germany, October 10-11, 2011.

[6] Oracle. (November 2011). System Administration Guide: Security Services. [Online]. Available: http://docs.oracle.com/cd/E19963-01/html/821-1456/concept-1.html

[7] N. T. Abdelmajid, M. A. Hossain, S. Shepherd, and K. Mahmoud, "Location-Based Kerberos Authentication Protocol," in *Proc. IEEE Second International Conference On Social Computing (SosialCom)*, 20-22 August, 2010, pp. 1099-1104.

[8] S. E. Hallyn. Role-based access control in SElinux. *IBM*. [Online]. Available :http//www.ibm.com/developerworks/library/l-rbac-selinux

[9] A. Armando, R. Carbone, and S. Ranise, "Automated Analysis of Semantic-Aware Access Control Policies: a Logic-Based Approach," in *Proc. Fifth IEEE International Conference on Semantic Computing*, 2011.

[10] A. Rosenthal, L. Seligman, and A. Chapman, "Barbara Blaustein, Scalable Access Controls for lineage," in *Proc. TAPP09 First Workshop on Theory and Practice of Provenance*.

[11] TechTarget. Role-based access control: Pros of an open source RBAC implementation. [Online]. Available http://searchsecurity.techtarget.com/tip/Role-based-access-control-Pros-of-an-open-source-RBAC-implementation.

[12] K.-Q. Guan, H.-X. Li, and X.-L. Kong, "Application of RBAC Model in System Kernel," *TELKOMNIK*A, vol. 10, no. 7, pp. 1541-1546, November 2012.

[13] Y. Yang, J.-K. Ding, Q.-Y. Wen, and H. Zhang, "Research and Design of the PMI-Based Access Control Model for OpenVPN," in *Proc. AIAI International Conference on Advanced Intelligence and Awarenss Internet*, 2010, pp.77-80.

[14] R. Boutaba, W. Ng, and L.-G. Alberto, "Web-Based Customer Management of VPNs," *Journal of Network and Systems Managemen*t, vol. 9, issue 1, pp. 67-87, March, 2001.

[15] H. Schroeder, "VPN resource connectivity in large-scale enterprise networks," US Patent 8443435 B1, May 14, 2013.

Sharipah Setapa has received her degree in bachelor of computer and communication engineering from UniversitiSains Malaysia (USM), Malaysia in 1991. She has experience almost 10 years in the area of security. She currently working in MIMOS Berhad.

Tengku Puteri Suhilah has received her degree in bachelor of computer science from UniversitiTeknologi Malaysia (UTM), Malaysia in 1997. She has experience as a software developer for 6 years and as a business analyst for 5 years. She is currently working in MIMOS Berhad.