International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 6 Issue 9, September - 2022, Pages: 46-50

Analysis of A Role-Based Access Control for Information System

Dilnoza Sodikova [1] and Muborak Abduvaliyeva[2]

[1]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Cybersecurity and Criminology department Tashkent, Uzbekistan
Dilnoza_9517@mail.ru
[2]Nurafshon branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Department of international cooperation Tashkent, Uzbekistan
muborakvositzonova@gmail.com

Abstract— *Many industries have implemented access control lists. This concept can be used to manage user authorization in a large organization. It can be based on a standard role-based access control (RBAC) or other equivalent. Role access control lists are developed together with modules such as identification, authentication, authorization and auditing that can make the system efficient. Defining roles helps define each task correctly to avoid conflicts when the system is installed. After identification is provided, the system authenticates using a secure database based on active directory or software hardware. Strong authentication and encrypted role-based login and usage help increase user confidence in the system. The database may be located on the same system or elsewhere. The structure of the access control list and the relationship with the database determine the efficiency and performance of the system. After the system is operational, an audit trail is provided to verify all processing and actions. A good policy defines the correct approach to a specific task. Role and policy management helps implement access control lists in a way designed to reduce potential risks and vulnerabilities through network deployment or VPN workflow. This article further discusses architecture, design, and policy through observations and recommendations for improving access management maturity in an organization.*

Keywords— Access control list, role, security, structure

1. INTRODUCTION

The Internet is a convenient tool for data transfer and communication, and in recent times it has become like a cloud, where information is available at any time and can be accessed by anyone. Then came the term access control list to restrict access. It helps by restricting content, granting user permissions and managing traffic flow. An access control list can also block communication between computers through hardware devices or software. This is necessary because it can provide a level of protection and confidence to the data owner and the organization.

Another function of an access control list is to control network traffic on a router interface. A router is used to inspect, block, or redirect access to a packet. Traditionally, system and application permissions are controlled by a group. Application, permission and group membership are assigned by the system administrator. The system owner allows the user to access the application. It acts like a conduit that protects your data from falling into the hands of another party. When an organization is large, access control lists can be difficult to maintain, implement, and manage. Based on the National Institute of Standards and Technology (NIST), an access control list, namely Role-Based Access Control (RBAC), is the dominant model for advanced access control in large enterprises [1]. Traditional access control lists and RBAC have one common goal, at least to provide security.

2. METHODOLOGY

Different organizations may have different roles, actions, resource hierarchies and activities. In order to correctly define the role in the organization, it is necessary to know the functioning of the organization, the structure, the resource hierarchy and how the operations are carried out in it. The role should be viewed from a business perspective and then linked to policy. These policies explain which application is allowed for which task, resource list, or role. An access control map is created for each job function, such as role and permission [2]. The role changes when the user moves to another location or country, but he can perform the same operation with greater coverage.

To avoid conflicts, user database information must be updated synchronously with the access control list system. When the roles are partially defined, the system and the organization will be ineffective. Role mining helps extract useful information about a role based on a resource. Without a clear description of roles and a list of resources, the built system loses certain criteria of the organization.

3. ROLE BASED ACCESS CONTROL

The role-based method is designed to authorize users only with specific tasks and actions. RBAC is a flexible access to implement discretionary access control (DAC) or mandatory access control (MAC), which is a traditional access control list. Without a proper

standard structure, integration, maintenance and scalability will be difficult. Table 1 shows a comparison between them [3]. Traditional access control lists are assigned only to low-level data. Authorization and justification in RBAC during the operation ensures that the resource is assigned correctly. A company with many employees uses a role to restrict access. It is also known as role-based security and this role can be summarized as shown in Fig. 1.

Table 1: 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 administrated	Administrated 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

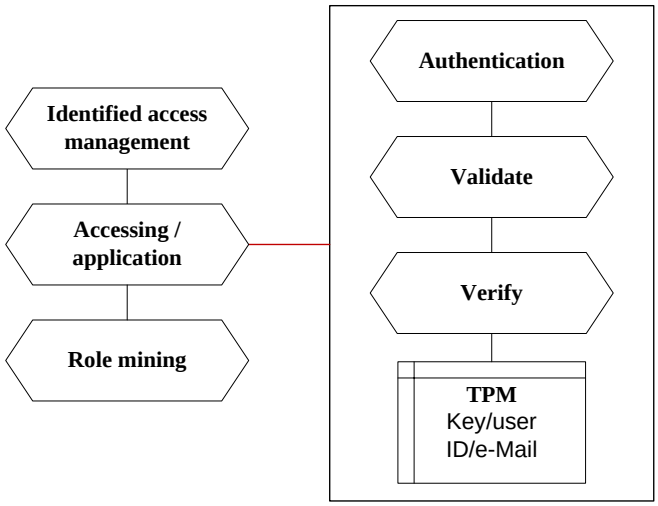

Fig. 1. *Role based security*

Verification and validation is based on the information in the database. This information can be an email address, an employee ID, and a pre-shared key. It is recommended to use another trusted key, such as the TPM key that comes with the TPM chip. It is recommended to take the baseline measurement stored in the Platform Configuration Register (PCR) as a benchmark for integrity measurement. Basic measurement can also be done without TPM by storing the measurement in a secure database. If the measurement matches, the check fails. All of this information must be communicated to the employee to ensure that verification and validation are successful.

The main step of the RBAC-based system (Fig. 2) can be described below:

1) Authentication is based on any token, credential, or employee-based information.

2) After successful authentication, login is allowed.

3) If the user is authorized based on previously defined policies for each resource, the operation can be performed.

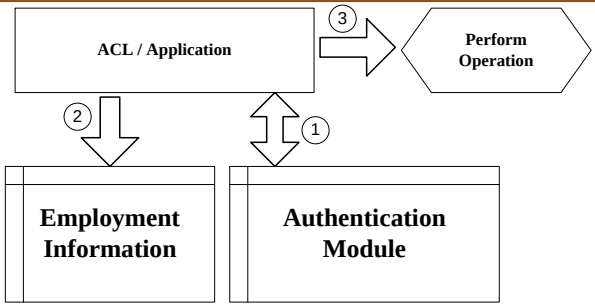

Fig. 2. *Basic step*

Each employee has their own duties depending on their duties. In some cases, an employee may have multiple roles as assigned by their supervisor. Assigning employees to multiple roles requires one end user. Three basic rules are defined for role control or RBAC [4]:

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

When assigning roles, the system administrator has the final privileges to assign a user to a role in the system. He can assign any role to anyone. When a role is assigned, they are granted permission. He may approve or disapprove any subject under his jurisdiction.

A set of permissions with different privileges allows different roles to be added to the system. There are many databases that support RBAC, including Microsoft Active Directory, Microsoft SQL Server, PostgreSQL, and SAP. The alignment of the data worker must be synchronized with the parameter in the application. If the data is missing or not updated in the database, the access control list will not show the user's exact data. Performance or response time is based on how the database is allocated or organized. The performance of this database can be affected by other components in the network infrastructure.

Administrative and management privileges through a single application is a best practice, as it reduces employee downtime, enables effective management of access control policies. In the backend process, it is necessary to learn the connection between the database and the application. For the transition to the system, the roles of the employees and the data structure must be clear and compatible with the system and vice versa [4, 5]. Without this, a conflict occurs during authentication and authorization for each role. Data management, downtime, ease of use, flexibility, and scalability are key criteria for developing a better access control list.

A role part can be created using different databases or the same database with user data. It can be done if the user database can match the role and resource, but it depends on the flexibility of software, hardware and hard disk space.

4. DISCUSSION

For a role-based access system, it must have security features to protect against intruders, which are: [6]:

- Authentication services - to securely identify a user that requires a username and some proof.
- Authentication with encryption - the ability to ensure that authenticated parties communicate without interception, alteration or forgery
- Auditing is the ability to identify the source of security changes to a system, including access security policies

Authentication is done to verify that the user is logged in correctly. This transmission is necessary to ensure verification from the database. Unfortunately, the transmission between authentications is not encrypted. If not encrypted, user data can be sniffed and seen in clear text.

Each time after logging out, the same process happens for logging in. If users do not want to change frequently, the same password and username are given. A smart password containing numbers, uppercase or lowercase letters is recommended. At this stage it is static because it is up to the user to change the password. This traditional authentication can be considered static rather than dynamic. Other authentication, such as Kerberos, provides a ticket to access certain applications or services. When buying a ticket, the user submits an application before receiving the ticket [7]. Although this method looks powerful, but it can be sniffed by modern hacking technology.

Using email for authentication has a vulnerability. If employees change email without notifying management, the database will not be updated. This causes access control to fail. As a result, someone can use the previous authentication to log in. Another question that needs to be clarified is how to manage multiple emails in the system. Employees who do not belong to the organization are advised to delete their e-mail from the database as soon as possible.

Role mining helps to learn a single role that has multiple policies. Some other policies are applied by other roles to access resources. Other roles are allowed to authorize by combining specific policies with other roles. Role duplication can be reduced through role mining. A new security module can be added under access/privileges. In a real organization with large staff, each employee has multiple roles. The role name and assignment is to implement the security policy.

A discussion is needed to define and analyze the role in a particular organization. It cannot be detected in a short time. The compiled system did not produce the expected result because the resource list and role were not obtained correctly [9]. When a role is analyzed, an expert from the business organization should work with the IT person to clarify it. It helps to convert the role to System.

5. Comparison Open Source and Commercial Product Scalability

It is difficult to compare an open source product to a commercial product supported by a graphical user interface. As with any other open source product, community support is strong to enhance the implementation [11]. Implementation of selection as a target policy. The role is then grouped into a domain. If domains A and B belong to role C, then a transition rule from domain A to domain B must be created to transition to domain B. SELinux is one example that uses the RBAC concept [8]. This RBAC is application based. Another RBAC for the device is called the core-RBAC model. This is one of the ways to protect the kernel under different operating systems [12]. This increases the security of the installed device.

Table 2: 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

In the process of working in an organization, our role as an employee can be that of a system administrator, a regular user, or a super administrator. Employees with super admins can access the full program, while regular employees have limited programs and resources. This is based on the rules or policies that apply to the application. Ontology occurs when role association and mapping is not easy. These lead to difficulties in assigning it by the system administrator. Group, application, and role are standard role controls. Each role management has this concept [8], but after this standard is implemented in the organization, some modifications or additional modules can be added to suit the organization structure. Usually, during our study, the standard does not completely match the environment of the organization. Without it, the system looks like a simple standard access control list without organization behavior. The first step in building a system is to obtain a firm requirement that will be affected by the organizational structure. Only in this case the system can be fully used.

A role can be filtered by all roles, single roles, and multiple roles. Role 1 can match resource 1. However, role 2 also needs a resource based on role 1. Filtering techniques can be based on a data-driven expert system or authorization rules. Filtering techniques can be knowledge-based or rules that match the appropriate resource for each role. As shown in Fig. 3, this can be useful when one role needs to access other resources that belong to another role by default.

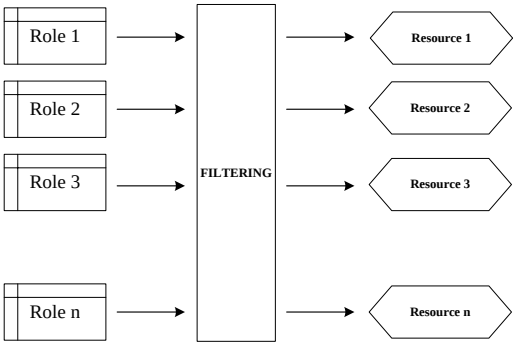

Fig. 3. *Connection of roles and resource*

The policy and role are based on the business order. Once the role condition is met, the policy must be checked. If the security policy is met, the condition for the role is met. From there, security policies are applied to ensure access to resources for the role. A role is an element that implements access to programs and resources. In order to create a security policy and security role, the system administrator must understand the relationship between role and role. Depending on the organization, the policy may have several terms. The source on the network accessed via a Virtual Private Network (VPN) is not controlled by the established tunnel. VPN only records the workflow. This policy and role can be included in the VPN flow to protect the resource from unauthorized access. Although it seems impossible, by setting up pre-defined roles and policies, it provides two layers of security in VPN [13]-[15].

6. CONCLUSION

Role and access controls are important to protect against misuse of resources in an organization. A resource accessed from an external organization using a VPN must have access control installed. Adding network access control protects against viruses or misuse of resources. This can be done by adding another process to the VPN workflow. The workload is increased to design a system that uses existing infrastructure.

7. 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] Irgasheva D., Khurramov D., Rustamova S. Approaches to Formalizing the Access Control System //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – C. 1-4.

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

[4] Irgasheva D. Indicators of Efficiency of Synthesis of Access Control Systems //2021 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2021. – C. 1-4.

[5] Irgasheva D. On the Basic Method for Solving the Problem of Synthesizing Access Control Systems //2020 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2020. – C. 1-4.

[6] Oracle System Administration Guide: Security Services. 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. Available :http//www.ibm.com/developerworks/library/l-rbac-selinux

[9] Irgasheva D., Rustamova S. Development of role model for computer system security //2019 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2019. – C. 1-5.

[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-Pro s-of-an-open-source-RBAC-implementation

[12] K.-Q. Guan, H.-X. Li, and X.-L. Kong, "Application of RBAC Model in System Kernel," TELKOMNIKA, 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. AI 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 Management, 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.