International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-7, July 2015

Secure Role Based Access Control

Indraja Salunkhe, Prof. Shailaja Gogate

***Abstract*— An organizations' business success comes when it is able to protect its data and assure its users that their data is always secure. To ensure this, the data is protected from most hostile environment round the clock. Protecting data can be costly and also must have security components that are easy to manage. RBAC provides the way to ensure that security administration is easy, flexible and efficient.**

RBAC (Role Based Access Control) describes an abstract pattern for level wise security. Roles given can be static as well as dynamic. Static roles never change thus blocking the flexibility function. Dynamic roles allow certain privileges to be overruled for certain amount of time. But this can only be done when and only when admin is available.

But when admin is not available; this paper enhances the ability of RBAC in real time to provide more options to administrator as well as users. Adding fuzzy logic to the current scenario of RBAC takes security to next level.

This paper describes the basic idea of how it can be implemented.

***Index Terms*— RBAC, fuzzy logic, security.**

I. INTRODUCTION

In this internet age, every service is made available online for user. The data and resources are distributed widely geographically. Therefore to manage the access to the data from the database over such a wide area is seen as a challenge. Privacy of data and Authorized access to resources are the two main concerns of any organization.

Many organizations still rely on individual, user-based identity management mechanisms built into the operating system and individual software applications. However, as the number of users and applications increase, supporting such a system becomes time-consuming, unwieldy and expensive.

MAC [1] and DAC [1] are the two main models for security. The Mandatory access Control is the method is used by military and civilian government. MAC enforces security labels to every object and user. A user is allowed to read an object only if he is labelled to do so The second model, Discretionary Access Control is the method is used in academic area. DAC allows the user to have control on permissions on object unlike MAC. A user is allowed to read an object if he is granted permission for it. A classical example of DAC is Access Control Lists (ACL) [1], where objects are associated with a list of users or groups that are allowed access.

The best solution to add flexibility to the current two models is done by RBAC.

Role based Access Control: A flexible model for controlling resources and enforcing organizational policies.

In this paper we will discuss the existing systems, our proposed model and its advantages.

II. LITERATURE SURVEY

[1]Security is Fuzzy! By H.Hosmer

In this paper, Hosmer states that "It is easier to use tools designed to deal with fuzziness than search in vain for the illusive perfectly secure system". It means any humanistic system is governed with imprecise perception. In the world of computer systems, where accuracy always comes first, Hosmer points the fact that it is not the same with systems that are human in nature. For example, if a system is designed to help a human to decide his job selection option; it is in the nature of system to be random and not accurate. System cannot define for sure that a certain job profile is perfect. The factors like job time, opportunities and progress and also salary issues.

[2] A Fuzzy Logic Approach for Remote Healthcare Monitoring by Learning and Recognizing Human Activities of Daily Living by Hamid Medjahed, Dan Istrate1, Jérôme Boudy, Jean Louis Baldinger, Lamine Bougueroua, Mohamed Achraf Dhouib and Bernadette Dorizzi

In this paper, the authors describe how pattern recognition in systems can help in plotting or collecting related data for the use of humanistic systems. The paper talks about data fusion which is a combination of characteristic of data and the fuzziness associated with it. Data characteristics can be measurement obtained from different readings and fuzziness can be the intelligence. Attribute representation, data description, analysis, clustering data and design are the steps to get pattern for decisions.

[3] Multicriteria Security System Performance Assessment Using Fuzzy Logic by William L. McGill, Bilal M. Ayyub

In this paper," Modern security problems focus on sensibly allocating resources to decrease the magnitude of potential adverse events (e.g., malicious attack), decrease the chances of perpetrator success given an attempt, or minimize loss following a successful incident" is the motto. This paper gives a brief description about securing a system using the formula:

Risk= threat x vulnerability x consequence

Where:

Threat: describes a set of adverse initiating events

Vulnerability: comprises a set of system or target weaknesses (e.g., security, hardness) that can be exploited by an adversary to achieve a given degree of loss or harm.

Consequence: describes the spectrum of losses that can felt by the victims following their occurrence.

CARVER: Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognisability. This method gives the idea of vulnerable points in a system.

III. RBAC

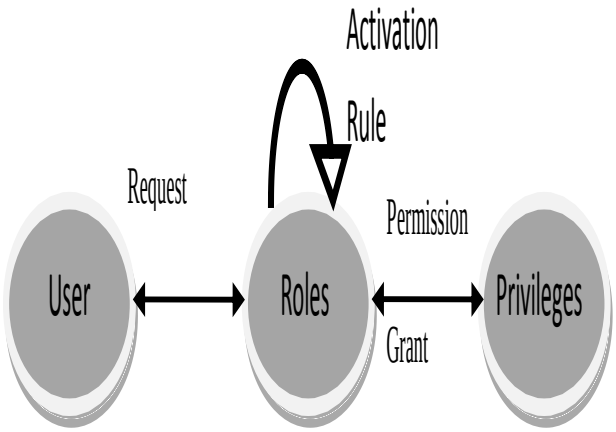

Figure No.1 RBAC Functioning basics

The above diagram shows how roles are assigned to each user with an activation rule. These rules are set by the admin in order to maintain a proper hierarchical security layer.

* Advantages of RBAC:

1. Role specific privileges
2. Regulatory control of integrity and confidentiality
3. Low maintenance cost
4. Tracks specific user activity
5. Maximises operational performance
6. Roles can be centrally managed

* Difference between RBAC and ACL (Access Control Lists) / DAC

1. RBAC: Easy management; ACL: Hard to Manage
2. RBAC: Group level permissions; ACL: personal permissions
3. RBAC: Set by system owner; ACL: set by data owner
4. RBAC: It has Role+Privileges; ACL: It has Role+Resource
5. RBAC: Defines 'Who has Access to my data'; ACL: Defines 'What the user can do'

* Security Problems in RBAC:

Using roles, companies can maintain a consistent security posture, audit the accuracy of access, prevent "access creep" and effectively manage thousands of users and rapid change. For all the value of role-based access control however, security professionals may find it difficult to design good RBAC models for a company. The problem lies in role engineering. Role engineering is the selection of appropriate roles, design of a role hierarchy that matches the corporate culture, and structure and management of roles as the company changes. These are all organizational, process and operational challenges – all things outside the core skill set of security pros and extending far beyond IT. Role-based access management is at its core a business issue, not a technology issue. The admin may be able to assign roles properly to the system. There may be common "core" roles shared by most employees within a department. For example, in an educational environment, core roles might include "student" and "staff." Almost immediately, you will see that even at the simplest level there will be exceptions: Is a lab assistant a student or a member of staff, or both? These types of cases will lead to the definition of more specific roles that can be "layered" to create a complex set of permissions. For example, a lab assistant may have the "student" role, the "student advisor" role and the "lab manager" role. A member of staff may have the "staff" role and the "lab manager" role.

Consider an example 1; a new employee is recruited in a company XYZ Pvt Ltd. Priya is at the post of HR. She has to add the details of the new employee to the main database O. The admin of the database Rushabh is on leave. Priya has only the permission to view any database entries. She has no right to update or add new employee details. This flaw can cause limitations in the functioning of the recruitment process and may delay it. Also, if there are any important transactions to be done on that day Priya may not be able to do it because she does not have access.

The current system follows DAC which is limited to certain conditions where user is allowed to use a specific list of resources.

The security parameter is also at stake because the role hierarchies that can ease the system functionality can also create a lot of confusion. So, SRBAC provides a solution for it.

In the next section, we define a way to formulate flexible RBAC with additional security provided by Fuzzy Logic. This technique is not yet researched to its full extent but we would want to put light on the topic. Any systems that always ask for definite fixed answers will not last long in terms of agility. The answer may then may be close to or almost correct just as a human behaviour.

IV. FUZZY LOGIC AND RBAC

1. Fuzzy Logic

A logic that deals with approximate value rather than exact value. The traditional value is either 1 or 0. Fuzzy logic values are between 0 to 1. These values help us to form a group or a range in which objects can be categorized.

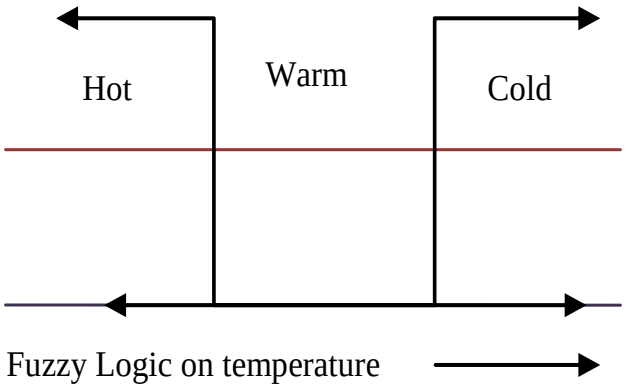

Fig no.2 depicting water temperatures in fuzzy sets

The above example shows that if a temperature is changed after certain limits, it can be a mixture of the two elements. There can be two sets: HOT () and COLD (), and an intersection H U C () set. Rather than an accurate value about when the water exactly turns from hot to warm or from cold to warm is defined by these sets.

2. Fuzzy logic and RBAC = Secure RBAC

In most of the organizations, roles and permissions to the system are assigned by system admin. But it has been seen from last few years that suppose any employee is absent and company needs someone to handle his task, RBAC does not provide any help for it. The solution followed is one has to call absent employee ask his login credentials and start working using his credentials. This solution is very unsafe and can be misused by hackers or attackers to harm company. Same problem is faced by Cognifront which is solved using Secure RBAC. Secure RBAC works on four steps. For any user to get role of other user he needs to clear first three steps. Fourth step is necessary for execution (COMMIT) of changes or work done. All steps are as follows:

1. Requested Role Verification
2. User System Verification
3. Fuzzy questions to verify user
4. Final Execution.

A. Requested Role Verification:

This is basic and most important step in Secure RBAC. In this we check whether we should allow user to use requested role by comparing his role and requested role. The reason behind doing this is simple we cannot grant very high role to very low role user.

Let us understand this with example. Suppose a team is working on project consisting of two programmers. Both have implemented the given task and now it's time to combine both works. But today one programmer is absent and project leader wants to see combine module today itself. So other programmer wants to access code of absent programmer so he makes request to Secure RBAC. So here SRBAC will check requested role which is programmer and role of user requesting is also programmer. In this case SRBAC will clear the request as both roles are same. In other case if Programmer is asking for a role of CEO then it will not allow it, only CMO or Director can be granted CEO role.

So SRBAC maintains database like relations wherein it is defined which roles are linked. So when anyone requests for role it is checked whether that role is linked with user role. If role is linked RBAC goes to next step else request is rejected in first step itself.

B. User System Verification:

So once user clears first step it has to deal with most critical step. Here SRBAC verifies the system from which the user is requesting

for role permission. It is necessary to check that system belongs to companies registered systems only.

For this we are making use of two inbuilt features of PHP. First with the help of user_agent all possible date is collected in PHP. Then to get more details we use service of www.ipaddresslocation.org by using CURL in PHP. When user opens the Cognifront website his data is fetched using user_agent and then his ip is directed to ipaddresslocation.org to fetch other details. The following details are extracted:

- *IP*
- *HostName*
- *Country*
- *Country Code*
- *Continent* State
- Latitude
- Longitude
- ISP
- OS
- Browser

The above details are checked with registered systems if record is matched then user proceeds to third step. But it also takes care if system is not from registered users. In such case it sends a random password to requesting user email or phone. So using that password one can clear second step. Basic aim of this step is to verify that the person requesting for role is not attacker.

C. Fuzzy Questions:

This step checks that the user belongs to company only and is not outsider or attacker. Once user clears first two steps he is provided with random questions which are already stored in database. Five to Ten questions are asked depending upon the requested role. If Requested role is very important more questions are asked. SRBAC takes care that the questions which are asked cannot be easily found on internet.

Following are simple but tricky questions that are known by company employee only. The questions are:

- What is your mother's name?
- How many rooms are there in your office?
- How many kids does your Director have?
- Where last Trip Company had gone?
- What current version of OS used by Company?
- Which company chairs are used in Company?

All the activities done by user are considered to be temporary execution. If user is able to answer these questions then only he is granted the requested role for certain period of time. If user is unable to answer then alarm is sent to information security officer so that he can investigate the problem.

If user clears all three steps he gets the requested role for certain time and a notification is sent to employee whose role is used by user. The user/employee can perform the work using that role.

D. Final Execution:

The last step is for the employee or person whose role was used when he was not present. When he again joins the company next day and login into his account he will get immediate pop-up about all the activities done by other employee in his absence. He will check all activities and decide whether to commit those activities or rollback all work done after inspecting it.

Advantages of this system: This system minimises the necessity of checking the user for authority in case the admin is unavailable. The admin can come back and check all the details of the user's machine and then can wither commit the details of transaction or rollback on old database. This can save a lot of time and makes the system secure.

V. CONCLUSION

Though RBAC provides the easy way to apply roles to their respective privileges, security was an important issue to

handle. SRBAC is devised to handle that problem. SRBAC describes a way to allow users to access and continue their transactions in case the admin is not available. This makes the module flexible than RBAC.

ACKNOWLEDGMENT

We would like to thank our supporters, contributors, friends and colleagues who have encouraged us to keep innovating. We would like to thank our professors for their constant guidance.

REFERENCES

[1] Hilary H. Homer, "SECURITYISFUZZY! Applying the Fuzzy Logic Paradigm to the Multipolicy Paradigm", Data Security Inc, 1993.

[2] Hamid Medjahed, Dan Istrate1, Jérôme Boudy, Jean Louis Baldinger, Lamine Bougueroua, Mohamed Achraf Dhouib and Bernadette Dorizzi, "A Fuzzy Logic Approach for Remote Healthcare Monitoring by Learning and Recognizing Human Activities of Daily Living", ESIGETEL-LRIT, Avon, 2Telecom SudParis, Evry, France,2012.

[3] Hamid Medjahed, Dan Istrate, Jérôme Boudy, Jean Louis Baldinger, Lamine Bougueroua, Mohamed Achraf Dhouib and Bernadette Dorizzi (2012), "A Fuzzy Logic Approach for Remote Healthcare Monitoring by Learning and Recognizing Human Activities of Daily Living, Fuzzy Logic - Emerging Technologies and Applications", ESIGETEL-LRIT, Avon, Telecom SudParis, Evry, France, 2012.

[4] Margaret Rouse, "Role Based Access Control (RBAC)" http://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC, 2008.

[5] Margaret Rouse,"Role Mining", http://searchsecurity.techtarget.com/definition/role-mining# ,2008.

[6] Hazen A. Weber , "SANS Institute InfoSec Reading Room", SANS institute, October 3rd 2003