भारतीय सूचना प्रौद्योगिकी संस्थान धारवाड़

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY DHARWAD

Data Base Management System Seminar Report

on

‘ACCESS CONTROL MODELS AND TECHNIQUES’

By:KapilJhade

Roll no: 17BCS013

Under the guidence of: Dr. Uma shadri

1. Introduction

1. Scope of the Topic:

Extra security of information and information systems is a basic management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include access control in some or the other form. Access control is concerned with determining the allowed activities of users, mediating every attempt by a user to access a resource in the system. Few systems are granted complete access after successful authentication of the user, there also exists systems that require more sophisticated and complex control. In addition to the authentication mechanism like password, access control is concerned with structuring of authorization. Authorization mirrors the structure of the organization.

Access control basically limit the actions or operations that a legitimate user of a computer system can perform. It constraints what a user can do directly, and also the programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of The access control may be based on different policies which in turn follows different principles. The choice of a security policy is important because it influences the flexibility, usability, and performance of the system.

The purpose of these researches is to provide background information on access control policies, models, and mechanisms to secure the computer applications. The papers that I have chosen discusses the capabilities, limitations, and qualities of the access control mechanisms that are embedded for each access control policy. They also provide a different Attribute based access control method say ABACα. There is also a sustainable access control model discussed in one of the paper.

2. Literature Study:

Starting from Lampson's access matrix in the late 1960's, dozens of access control models have been proposed. Only three have achieved success in practice: discretionary access control (DAC), mandatory access control (MAC, also known as lattice based access control or multilevel security) and role-based access control (RBAC). While DAC and MAC emerged in the early 1970's it took another quarter century for RBAC to develop robust foundations and flourish. RBAC emerged due to increasing practitioner dissatisfaction with the dominant DAC and MAC paradigms, inspiring academic research on RBAC. Since then RBAC has become the dominating form of access control methodologies. Recently there has been growing practitioner concern with the limitations of RBAC, which has been met by researchers in two different ways. On one hand researchers have diligently and creatively extended RBAC in numerous directions.
Conversely there is growing appreciation that a more general model, specifically attribute-based access control (ABAC), could encompass the demonstrated benefits of DAC, MAC and RBAC while transcending their limitations.

There also came Sustainable access control methodologies which helped excessively in privacy and security of data by providing one such very easy to use model that is further discussed in this document.

2. New proposed Solutions - Research papers

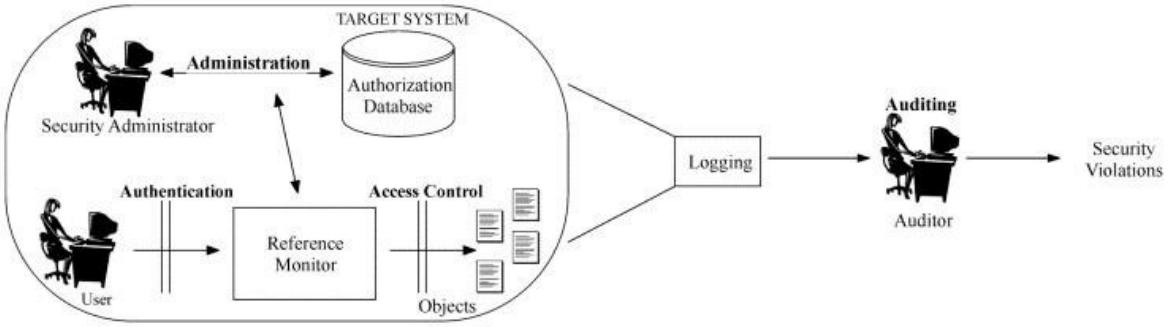
2.1 Paper 1: Database Security & Access Control Models: A Brief Overview

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

[Describe the proposed [prominent] solution , model, framework by the author with figures. Information should be limited to Maximum Two Pages]
There are three proposed Access Control models in this research paper:

1. DISCRETIONARY ACCESS CONTROL (DAC)

Specify the rules, under which subjects can, at their discretion, create and delete objects, and grant and revoke authorizations for accessing objects to others Govern the access of users to information on the basis of user's identity and predefined discretionary rules" defined by security administrator. The types of access the user is allowed for the object is specified in this rule. The request of a user to access an object is checked against the specified authorizations. if there exists an authorization stating that the user can access the object in the specific mode, the access is granted; otherwise it is denied. The policies are discretionary in that they allow users to grant other users authorizations to access the objects.



The System R Authorization Model:

This model is first defined by Griffiths and Wade, and later revised by Fagin. Possible relational databases privileges user can exercise on tables are select, insert, delete and update . The model supports decentralized administration of authorizations. Any database user is authorized to create a new table; once the table is created he becomes the owner of the table and is fully authorized to exercise all privileges on the table. The owner can also grant all privileges on the table to other users.

Extensions to the System R Model:

The two main extensions are as follows:
i. A new type of REVOKE operation, called non- cascading is introduced.
ii. The system R model uses closed world policy under which when a user tries to access a table and if positive authorization is not found, the user is denied access. The major problem with this approach is that a user does not guarantee that he will not acquire the authorization anytime in future. The use of explicit negative authorizations can overcome this drawback. According to which if a user has both negative and positive authorization for a

given privilege in the same table; the user is prevented from using the privilege on the table.

Trojan Horse Attacks:

A Trojan horse is a computer program which apparently or actually cointains useful function, it contains additional hidden functions that surreptitiously exploit the lawful authorizations of the invoking process. The Trojan Horse Attacks is explained in the research paper by the example of an organization where the sensitive information is stolen using this attack.

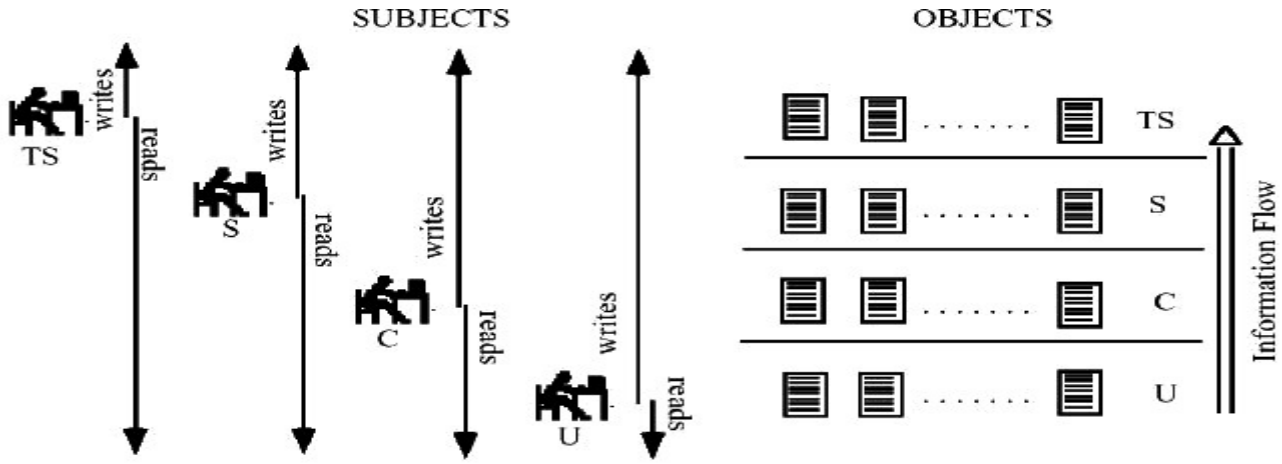
2. MANDATORY CONTROL (MAC):

MAC security policies govern the access on the basis of the classifications of subjects and objects in the system [6]. Objects are the passive entries storing information for example relations, tuples in a relation etc. Subjects are active entities that access the objects, usually, active processes operating on behalf of users.

Access control in mandatory protection systems is based on the following two principles: No read-up/ Read down: A subject can read only those objects whose access class is dominated by the access class of the subject.

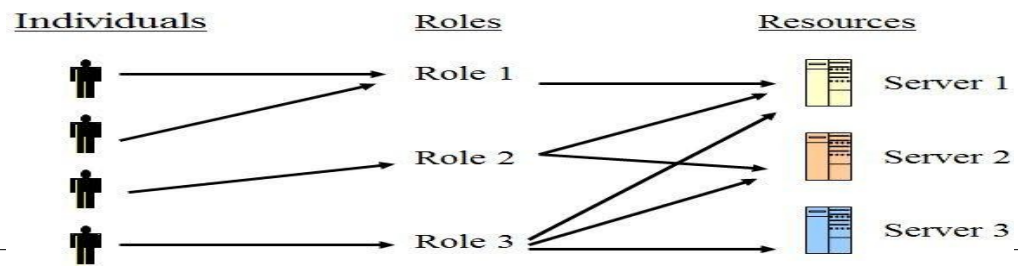
No write-down/Write up: A subject can write only those objects whose access class dominates the access class of the subject.

MAC models are not vulnerable to Trojan horse attacks.



3. ROLE – BASED CONTROL (RBAC)

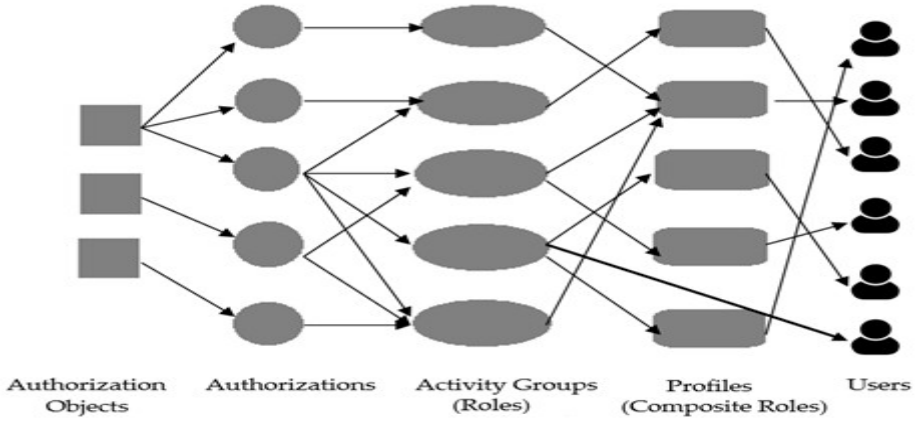
Role-based access control (RBAC), permissions are associated with some particular roles, and the users are made members of those roles . This method very well simplifies the management of permissions . Now these roles are closely related to different user groups for access control. Whereas, a role puts together the set of users on one side and the set of permissions on the other, however the user groups are defined as a set of users only.



2.2 Paper 2: Sustainable Implementation of Access Control

International Journal of Engineering Research & Technology (IJERT)
Received: 26 April 2018; Accepted: 29 May 2018; Published: 30 May 2018

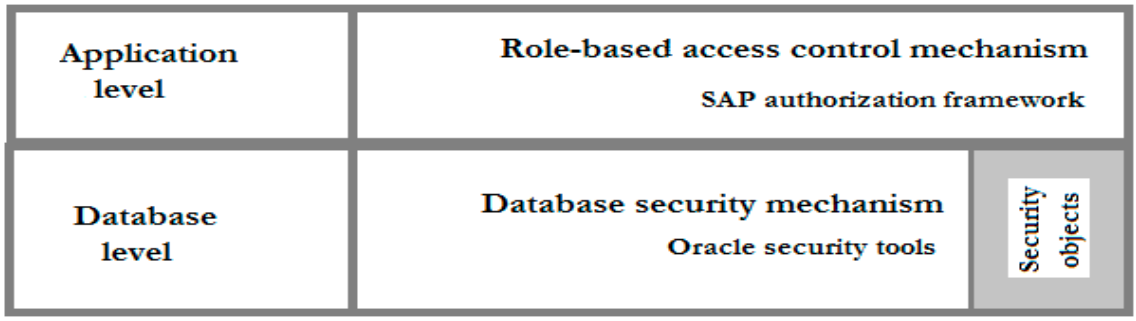
This research presents its own model for sustainable implementation of Access Control. They have identified four end-user categories: Information consumer/business user; business analyst/power user; middle management; and C-level management and leadership. Both authentication and access control of users are defined according to the authorization framework. In this SAP applications, authorizations are the key building blocks of SAP security. Business objects and the transactions in SAP are protected by authorization objects. Users require corresponding authorization to access the business objects/execute the transactions.
The authorization framework are involved in establishing the relationships between the users and the authorization objects.



Authorization framework

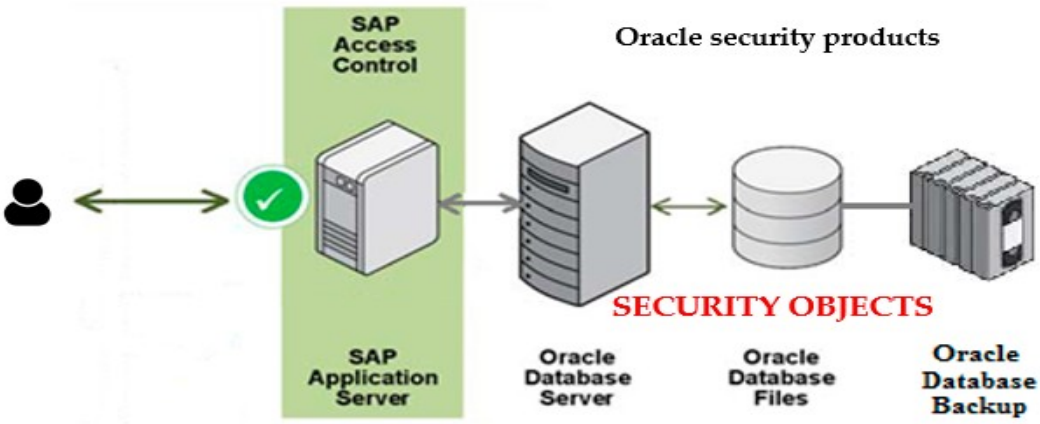
Sustainability is a new dimension of information system. .Users access is performed according to the security configurations in SAP. At application level, beyond the role-based access control mechanism the access to data at database level is also controlled. Oracles native security tools, like Oracle Advanced Security and Oracle database vault, are implied.

For monitoring users access, stored procedures are triggered in Oracle have been defined. Also a way of locking and unlocking users has been introduced at database level. The proposed stored procedure and triggers are programmed in the procedural language extension to structural query language (SQL). Due to their defined functionality they are referred as security objects in the present demarcha . A higher speed of monitoring process is achieved and troubleshooting intervention is more quickly possible. This contribution in defining the security objects is meant to minimize the chances of the system being exploited by the malicious users. The hybrid access control framework is based on a access control model at application level, native database security mechanism and the security objects. The security framework has been integrated into an ERP application which is already been put into operation.



Security Framework

SAP applications benefit from an authorization framework based on authorization objects, authorizations, roles and profiles. At database level, e.g., Oracle server offer security tools to protect the data. Best practices in Oracle security for SAP offer support in protecting the data, isolating, if necessary, the applications, limiting user and actions, and reporting on system activities. Any additional approach in consolidating a sustainable access control increases the robustness of the system. Thereby, the proposed demarche increases the capabilities of the overall security system.



Sustainable access control

2.3 Paper 3: A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC

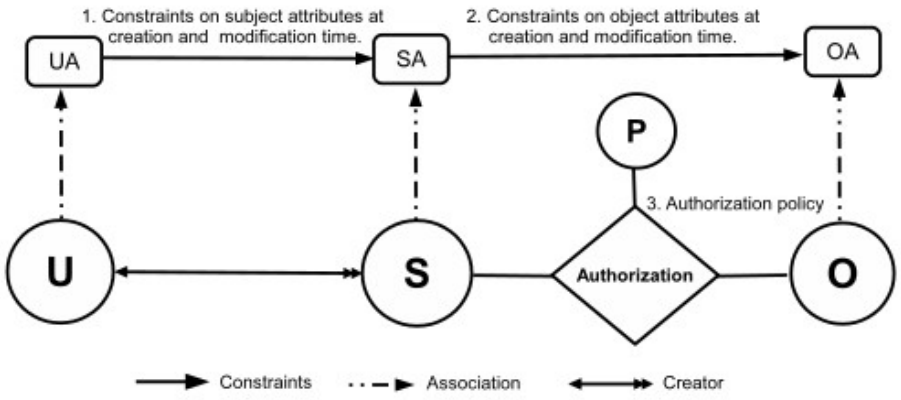
International Journal of Engineering Research & Technology (IJERT)
published: 13, April - 2015

In this paper, goal is to develop an authoritative family of foundational models for attribute based access control. this goal can be achieved only by means of incremental steps that advance our understanding. ABAC is a rich platform. It is infeasible to address it in its full scope from the beginning . There are simply too many moving parts. In the first step we develop a formal ABAC model that is just sufficiently expressive to capture DAC, MAC and RBAC. This provides a well-defined scope ensuring that the resulting model has practical relevance. There have been informal demonstrations, of the classical models using attributes. The goal is to develop more complete and formal constructions.

The goal was to develop an ABAC model that has “just sufficient” features to be “easily and naturally” configured to do DAC, MAC and RBAC. For clarity of reference model is designeted as ABAC α . Hence final goal is to eventually develop a family of ABAC models, analogous to RBAC, which will become the de facto standard for defining, refining and evolving ABAC.

A unified ABAC α model is presented informally The structure of ABAC α model is shown in Figure below. The core components of this model are: users (U), subjects (S), objects (O), user attributes (U A), subject attributes (SA), object attributes (OA), permissions (P), authorization policies, and constraint checking policies which are needed to create and modify subject and object attributes. An attribute is a function which takes an entity such as a user and returns a specific value from its range. An attribute range is given by a finite set of atomic46 values. An atomic valued attribute returns one value from the range, while a set valued attribute returns a subset of the range. Each user is associated with a finite set of user attribute functions and theirvvalues are assigned by security administrators (outside the scope of the model). These attributes represents the user properties, including name, clearance, roles and gender. Then the subjects are created by users to perform some actions in the system. For the purpose of this paper, subjects can only be created by a user and are not allowed to create other subjects. There is only one creating user who can terminate a subject. Each subject is associated with a finite set of subject attribute functions that is provided with an initial value at creation time. Subject attributes are then set by the creating user and are constrained by policies established by security architects (discussed later). For example, a subject attribute value may be inherited from any corresponding user attribute. This is shown in Figure as an arrow from user attributes to subject attributes. Objects are resources that need to be protected. Objects are matched with a finite set of object attribute functions. Objects may be created by a subject corresponding to its user. The object’s attribute values is set by the user via the subject at creation time. The values are constrained by the corresponding subject’s attributes. For example, the new object can inherit values from corresponding subject attributes. In Figure, the arrow from subject attributes to object attributes indicates this relationship.

ABAC α model and showed that it can be used to naturally configure the three classical models. This paper assist understanding the connections between desired ABAC model and widely-deployed classical models.



3. Glossary/References

Glossary:

RBAC: Role-based Access Control
ABAC: Attribute-based Access Control
MAC: Mandatory Access Control
DAC: Discretionary Access Control
CAC: Cryptographic Access Control
SAP: Sustanable Access Control

References:

1. https://www.ijert.org/research/database-security-access-control-models-a-brief-overview-IJERTV2IS50406.pdf
2. https://scinapse.io/papers/2097171586
3. https://scinapse.io/papers/2807504979