International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

ROLE-BASED ACCESS CONTROL APPROACH FOR APPLICATION LEVEL SECURITY AGAINST INSIDER ATTACKS

Nishi Jain, Dr. Neetu Sharma

M.Tech Scholar, Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Jhajjar Haryana (India),2019

Associate Professor, Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Jhajjar Haryana (India),2019

Insider attacks are a major issue now days. It is a worldwide concern. In a brief view, “insider” is a person who is engaged by a business and therefore has the chance to have a knowledge of some internal news or can access secret information or data. Compare with outsiders, insiders have better knowledge about how their system works and that is why insider attack may cause more hardazous than outsider attack. Bank security is important for a following of reasons; one of those reasons includes providing secure banking for customers and protecting the bank from unauthourized person. Intrusion detection systems have the task of observing the usage of application based systems to detect any manifestation of uncertain states. They find out attempts and active misuse either by authorized users of the information systems or by external parties to exploit their privileges or security vulnerabilities.

Access control can confined the information access to users. In order to grant the access of multiple user a role based access control approach was implemented. Instead of granting permission to each and every user a roles are defined based on the task positions a user has in an organization. Permission are granted to roles and roles are assigned to the user to perform certain task in the organization and access certain application. It is a way of restricted user to access only those information who have a previlleged.

ABBREVIATIONS

IDS -Intrusion Detection System, IPS.Intrusion Prevention System, IDPS-Intrusion Detection and Prevention System, IDR -Intrusion Detection and Response, NIDS -Network-based intrusion detection systems, HIDS-Host- based intrusion detection systems, RBAC-Role Based Access Control, ACL -Access Control List, UA-User Agent/Assignment, PA-Permission Assignment, RH-Role Hierarchy, OPS-Operations, AUA-Administrative User Assignment, AR-Administrative Role, ARH-Administrative Role Hierarchy, AP-Administrative Privilege, APA-Administrative Privilege Assignment, OTSK-One Time Security Key.

INTRODUCTION

1.1 About IDS

Now a days Data represent an important resource for companies and organizations. Organizations take great care at controlling access to these data with respect to both insider and outsiders because some of the data of an organizations are worth millions of dollars. Security of data is also crucial when addressing issues related to privacy of data referring to individuals; companies and organizations supervising such data need to provide strong guarantees about the confidentiality of these data.

Insider attacks are a major issue now days. It is a worldwide concern. In a brief view, “insider” is a person who is engaged by a business and therefore has the chance to have a knowledge of some internal news or can access secret information or data. Compare with outsiders, insiders have better knowledge about how their system works and that is why insider attack may cause more hardazous than outsider attack. In banking and finance sector mostly insiders (70%) committed acts while on the job; in contrast ex-employees was mainly performed by insider attack in computer system sabotage. and the majority of attacks took place outside normal working hours. Bank security is important for a following of reasons; one of those reasons includes providing secure banking for customers and protecting the bank from unauthourized person.

The main aim of Instrusion detection systems is to detect against computer systems and networks or,in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, the task of intrusion detection system to monitor the usage of such system and to detect any illusion of inseure states. They detect active misuse and attempt either by authorized users of the information systems or by external parties to misdeed their privileges or exploit security vulnerabilities.

The first area explored in intrusion detection was Host-based intrusion detection. When the first intrusion detection systems were designed, all users were local to the system considered and the target environment was a mainframe computer. The intrusion-detection system investigate the information provided by the mainframe, either locally or on a separate machine, and reported security-suspicious events.

1.2 About RBAC

Recently Role-based access control (RBAC) has received considerable attention as a promising alternative to traditional discretionary and mandatory access controls. In RBAC privileged are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' privileged. This greatly simplifies management of privileged. In an organization for the various job functions roles are created and users are assigned roles based on their work and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new privileged as new applications and systems are incorporated, and privileged can be revoked from roles as needed. In large organizations the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands. Administering these roles and users, and their interrelationships is a terrific task that often is highly centralized in a small team of security administrators.

There are many components to RBAC. RBAC administration is therefore complicated. In particular we can separate the issues of assigning users to roles, assigning privilege to roles, and assigning roles to roles to define a role hierarchy. These activities are all required to bring users and privileged together. However, in many cases, they are best done by different administrators or administrative roles.

Intrusion Detection System

2.1 Brief Description

Intrusion means to interrupt someone without permission. Intrusion is an attempt to use the resource of computer system without any privileged Intrusion Detection means any mechanism which detects frauldent behavior. Intrusion detection system (IDS) observe network traffic and its

suspicious behavior and if it detect any threat and vulnerable alert the system or network administrator. The main objective of IDS is to detect and inform about intrusions. An Intrusion Detection System have a set of techniques and methods that are used to find out suspicious activities both at the network and host level. There are two main types of intrusion detection system (IDS), host based intrusion detection systems (HIDS) and network based intrusion detection systems (NIDS).

2.2 Description of a generic intrusion-detection system

2.2.1 Terminology

The term system is used here to denote the information system being monitored by the intrusion-detection system. It can be a network element, a server, a firewall, a web server, a workstation, a mainframe etc. The term audit denotes information provided by a system concerning about its insider workings and behavior. An intrusion-detection system contained information about an information system to perform a analysis on the security status of the latter. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. A typical intrusion-detection system is shown in Figure1.

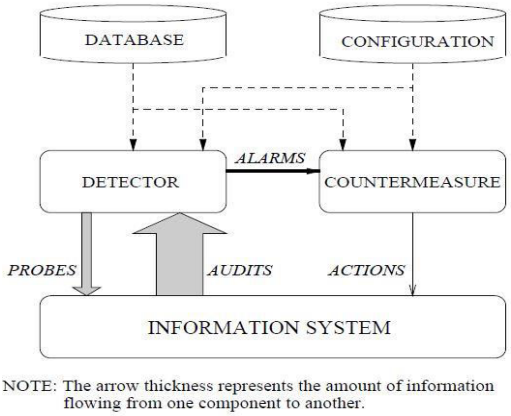

Figure 1: Very simple intrusion-detection system

An intrusion-detection system can be described at a very macroscopic level as a detector that processes the information coming from the system are to be protected.

2.3 Efficiency of intrusion-detection systems

Tthe efficiency of an intrusion-detection system, have proposed the following three parameters:

Accuracy: Accuracy is the parameter deals with the proper detection of attacks. Inaccuracy occurs when an intrusion-detection system flags a legitimate action in the intrusive environment.

Performance: The performance is the second parameter of an intrusion-detection system is the rate at which audit events are processed. If the performance of the IDS is poor, then real-time detection is not possible.

Completeness: Completeness is the third property of an intrusion-detection system is to detect all attacks. Incompleteness occurs when the intrusion-detection system fails to detect an attack.

Role-Based Access Control

3.1 The Purpose and Fundamentals of Access Control

Access control is one of the most important security features that have to be integrated into a secured environment of any organization. Access control is imposed, when a user logs in into the system which has multi-users. There are following three types of security risks.

- Confidentiality: It refers to keep the information or resources private and secure.
- Integrity: It refers to protecting information for unauthorized users.

- Availability: It refers to the information available for the use when needed.

3.2 The Role-Based Access Control Reference Model

The NIST RBAC model is defined in terms of four model components: Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations.

3.2.1. Core RBAC

Core RBAC includes sets of five basic data elements called users (USERS), roles (ROLES), objects (OBS), operations (OPS), and permissions (PRMS).The RBAC model is a model which fundamentally assign a role and assign a privileged to role. In addition the Core RBAC assign a session.

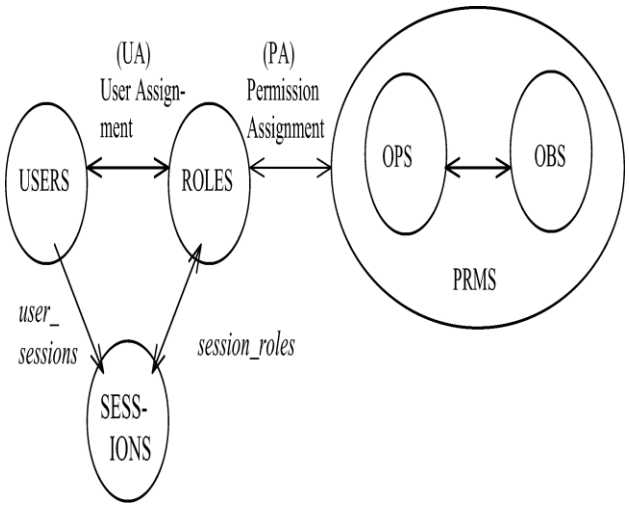

Figure. Core RBAC

3.2.2. Hierarchal RBAC

This model component introduces role hierarchies (RH). In Hierarchal RBAC key aspects are Role hierarchies. Role hierarchies define an inheritance relation among roles.

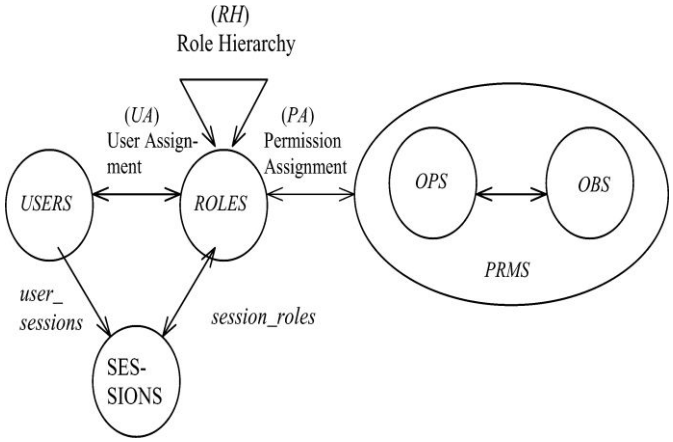

Figure Hierarchical RBAC

3.2.3 Constrained RBAC

Constrained RBAC is a RBAC model which separate of duty relations . Separation of duty relations are used to enforce conflict of interest policies that organizations may employ to prevent users from exceeding a reasonable level of authority for their positions and grant privileges according to their rules.

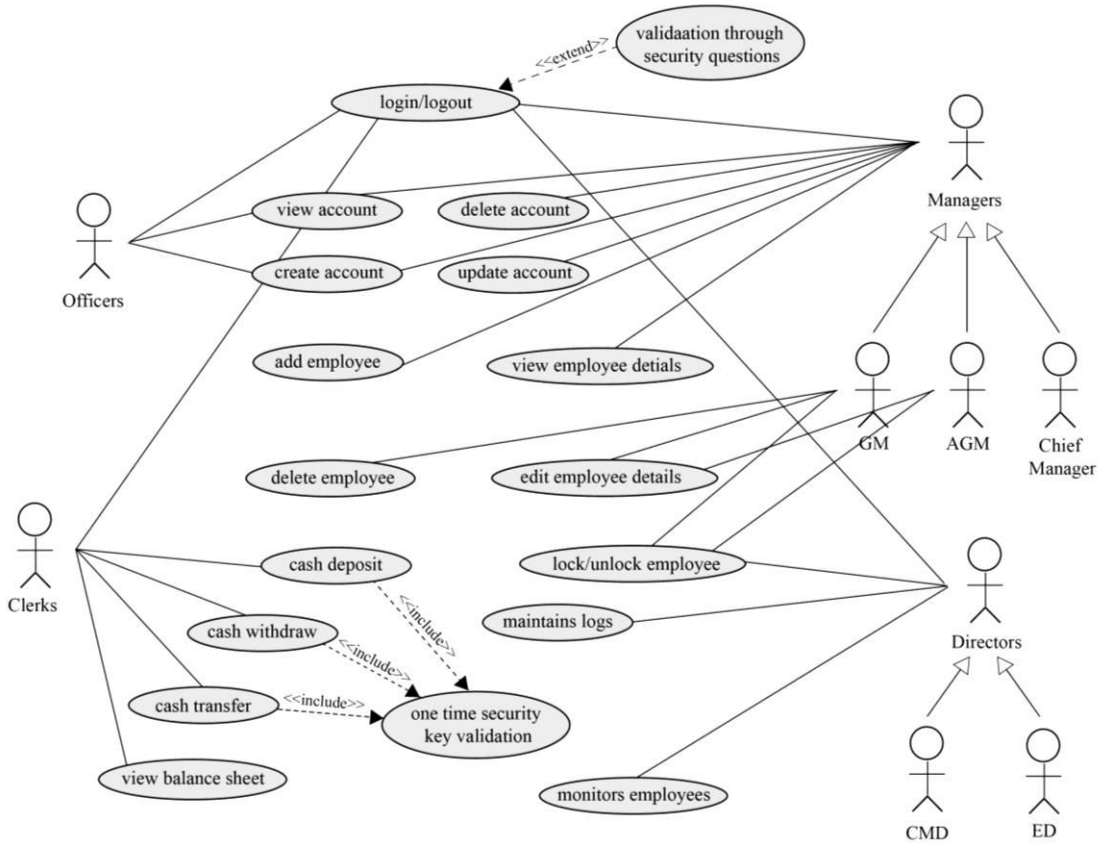

Figure . Constraint RBAC

Conclusion

The main goal of this dissertation is to build intrusion detection for relational databases integrated with the core database query processing mechanism. This project incorporated basic functionalities of Role-Based Access Control Model for an organization. The role is assigned based on the responsibilities the user share in an organization can only access the information, for which he/she is authorized. As a result, the security of the system will not be compromised by any malicious attacks on the system. All the necessary testing has been performed to test all kinds of scenarios to measure the security of an application. By implementing role-based access control, it has been proved that it is a really good solution for security purposes.

References

1.A. Anton, E.Bertino, N.Li, and T.Yu, “A roadmap for comprehensive online privacy policies,” in CERIAS Technical Report, 2004.

2.Herve Debar, IBM Research, Zurich Research, Laboratory, Saumerstrasse 4, CH8803 Ruschlikon, Switzerland, “An Introduction to Intrusion-Detection Systems”.

3.Teresa F. Lunt, R. Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann,Harold S. Javitz, and Alfonso Valdes. IDES: The enhanced prototype a real time intrusion detection expert system. Technical Report SRI-CSL-88-12, SRI International, 333 Ravenswood Avenue, Menlo Park, CA, October 1988.