International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

SOD Based Anomalous Detection Using JTAM

Nikhil Narayanan[1]

[1]Assistant Professor, UKF College of Engineering & Technology

---

Abstract - Database security is also a speciality within the broader discipline of computer security. Information is the most critical resource for many organizations. In many cases, the success of an organization depends on the availability of key information and therefore on the systems used to store and manage the data supporting that Information. Standard database security mechanisms such as access control, authentication and encryption are not of much help when it comes to preventing data theft from insiders. In Information Security intrusion detection is the act of detecting actions that attempt to compromise confidentiality, integrity, or availability of resource. When intrusion detection takes a preventive measure without direct human intervention, then it becomes an intrusion response system. In this, propose a novel Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty. The key idea in JTAM is that a policy object is jointly administered by at least k database administrator (DBAs) that is, any modification made to a policy object will be Invalid unless it has been authorized by at least k DBAs. In this for future enhancement present a high-level, informal overview

***Key Words*: SOD, JTAM, Intrusion Detection, Policy Matching, Policy Administration, Threshold Signature**

1. INTRODUCTION

ID mechanism consists of two main elements, specifically tailored to a DBMS: an anomaly detection (AD) system and an anomaly response system. The first element is based on the construction of database access profiles of roles and users, and on the use of such profiles for the A D task. A user-request that does not conform to the normal access profiles is characterized as anomalous. Profiles can record information of different levels of details. The second element of approach is the focus in charge of taking some actions once an anomaly is detected. There are three main types of response actions that refer to, respectively, as conservative actions, fine-grained actions, and aggressive actions. The conservative actions, such as sending an alert, allow the anomalous request to go through, whereas the aggressive actions can effectively block the anomalous request. Fine-grained response actions, on the other hand, are neither conservative nor aggressive. Such actions may suspend or taint an anomalous request. A suspended request is simply put on hold, until some specific actions are executed by the user, such as the execution of further authentication steps. A tainted request is marked as a potential suspicious request resulting in further monitoring of the user and possibly in the suspension or dropping of subsequent requests by the same user.

Attacks and Protection

In this describe possible attacks on JTAM and strategies to protect from them. Recall that the threat scenario that we address is that a DBA has all the privileges in the DBMS, and thus it is able to execute arbitrary SQL commands on the database.

Signature Share Verification

It is possible for a malicious administrator to replace a valid signature share with some other signature share that is generated on a different policy definition. However, such attack will fail as the final signature that is produced by the signature share combining algorithm will not be valid. Note that by submitting an invalid signature share, a malicious administrator can block the creation of a valid policy.

Final Signature Verification

Final signature on a policy is present in all the policy states except the CREATED state. The public key is assumed to be signed using a trusted third party certificate that cannot be forged. Thus, if a malicious DBA replaces the server generated public key, the final signature will be invalidated. Apart from verifying the final signature immediately after policy activation, suspension, and drop, the signature must also be verified before a policy may be considered in the policy matching procedure. Such strategy ensures that only the set of response policies, that have not been tampered, are considered for responding to an anomaly. Note that RSA signature verification requires modular exponentiation of the exponent e.

Malicious Policy Update

A policy may be modified by a malicious DBA using the SQL update statement. However, all policy definition attributes that need to be protected are hashed and signed; therefore any modification to such attributes through the SQL update command will invalidate the final signature on the policy.

Malicious Policy Deletion

An authorized policy may be deleted by a malicious DBA using the SQL delete command. However in JTAM, a policy tuple is never physically deleted; only its state is changed to DELETED. Thus, a signature on the policy-count can be used to detect malicious deletion of policy tuples. The detailed approach is as follows:

When the Create Response Policy command is executed; the DBMS counts the number policy after Final Authorization of Policy Suspension

1.1 Objective

The intrusion response component of an overall intrusion detection system is responsible for issuing a suitable response to an anomalous request. The notion of database response policies to support our intrusion response system tailored for a DBMS. Interactive response policy language makes it very easy for the database administrators to specify appropriate response actions for different circumstances depending upon the nature of the anomalous request. The two main issues that address in context of such response policies are that of policy matching, and policy administration.

In this propose two algorithms that efficiently search the policy database for policies that match an anomalous request. The main issue address is that of administration of response policies to prevent malicious modifications to policy objects from legitimate users. This method propose a novel Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty. The key idea in JTAM is that a policy object is jointly administered by at least k database administrator (DBAs), that is, any modification made to a policy object will be invalid unless it has been authorized by at least k DBAs.

1.2 Overview

The sensitive and proprietary data that is the real target of attackers Also , with greater data integration , aggregation and disclosure , preventing data theft , from both inside and outside organizations , has become a major challenge . Standard database security mechanisms, such as access control, authentication, and encryption, are not of much help when it comes to preventing data theft from insiders.

Such threats have thus forced organizations to reevaluate security strategies for their internal databases. Monitoring a database to detect potential intrusions, intrusion detection (ID), is a crucial technique that has to be part of any comprehensive security solution for high-assurance database security Note that the ID systems that are developed must be tailored for a Database Management System (DBMS) since database-related attacks such as SQL injection and data ex filtration are not malicious for the underlying operating system or the network. The main issue is essentially that of insider threats, that is, how to protect response policy object from malicious modifications made by a database user that has legimate access rights to the policy object.

1.2.1 Jtam Setup

Before the response policies can be used, some security parameters are registered with the DBMS as part of a onetime registration phase. The details of the registration phase are as follows: The parameter l is set equal to the number of DBAs registered with the DBMS. Such requirement allows any DBA to generate a valid signature share on a policy object, thereby making our approach very flexible. Shoup's scheme also requires a trusted dealer to generate the security parameters. This is because it relies on a special property of the RSA modulus, namely, that it must be the product of two safe primes. In this assume the DBMS to be the trusted component that generates the security parameters. For all values of k, such that the DBMS generates the following parameters.

RSA Public-Private Keys: The DBMS chooses p, q as two large prime numbers such that p=2p'+1 and q=2q'+1 ;where p' and q' are themselves large primes. Let n =p*q be the RSA modulus. Let m =p*q. The DBMS also chooses e as the RSA public exponent such that e >l. Thus, the RSA public key is PK = n(e). The server also computes the private key d eZ such that De= 1 mod m.

Threshold Signatures : A k out of l threshold signature scheme is a protocol that allows any subset of k users out of l users to generate a valid signature, but that disallows the creation of a valid signature if fewer than k users participate in the protocol. The basic paradigm of most well known threshold signature schemes is as follows : Each user Ui has a secret key share si corresponding to the signature key d. Each of the users Ui participating in the signature generation protocol generates a signature share that takes as input the message m (or the hash of the message) that needs to be signed, the secret key share si, and other public information. Signature shares from different users are then combined to form the final valid signature on m

1.2.2 Policy Matching

The policy matching algorithm is invoked when the response engine receives an anomaly detection assessment. For every attribute A in the anomaly assessment, the algorithm evaluates the predicates defined on A. After evaluating a predicate, the algorithm visits all the policy nodes connected to the evaluated predicate node. If the predicate evaluates to true, the algorithm increments the predicate-match-count of the connected policy nodes by one. A policy is matched when its predicate-match-count becomes equal to the number of predicates in the policy condition. On the other hand, if the predicate evaluates to false, the algorithm marks the connected policy nodes as invalidated. For every invalidated policy, the algorithm decrements the policy-match-count of the connected predicates; the rationale is that a predicate need not be evaluated if its policy-match count reaches zero. A response policy condition is a conjunction of predicates where each predicate is specified against a single anomaly attribute

1.2.3 Policy Administration

The policy creation command has the following format: Create Response Policy [Policy Data] Jointly Administered By k Users; Policy Data refers to the

interactive ECA response policy conditions and actions Suppose that DBA1 issues such command and that k= 3, and l = 5. DBA1 becomes the owner of the newly created policy object. The newly created policy will be administered by three users (including the owner). We define an administrator of a policy as a user that has owner-like privileges on the policy object. Owner-like privileges means that the user has all privileges on the object along with the ability to grant these privileges to other users.

Once the policy has been created, it must be authorized for activation by at least k _ 1 administrators after which the DBMS changes the state of the policy to ACTIVATED.

The policy activation command has the following format: Authorize Response Policy [Policy ID}_Create; Suppose that DBA3 issues such command. After the command is issued, the DBMS performs the following operations in a sequence

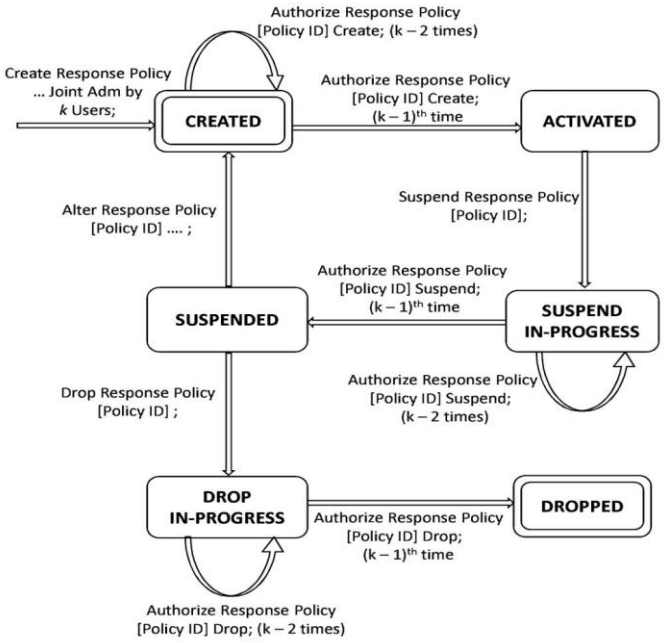

Fig-1: Policy State Transition Diagram

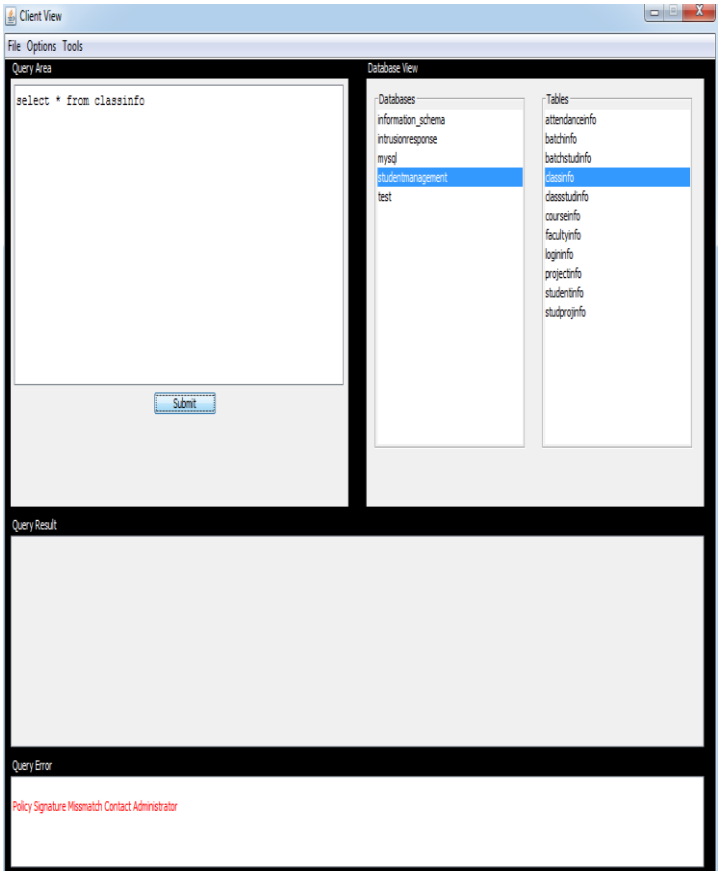

Figure 2: Policy Mismatching

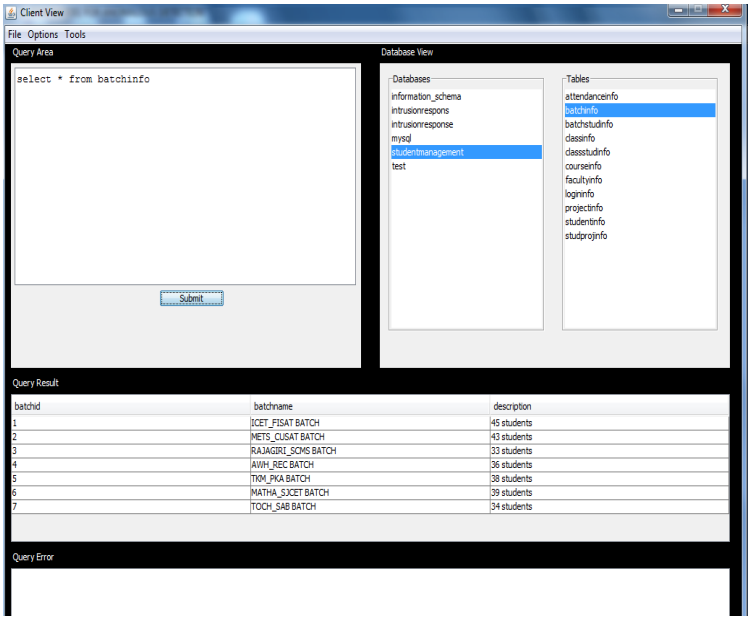

Fig-3: Privileged User

3. CONCLUSIONS

The intrusion response component of an overall intrusion detection system is responsible for issuing a suitable response to an anomalous request. The notion of database response policies to support our intrusion response system

tailored for a DBMS. Interactive response policy language makes it very easy for the database administrators to specify appropriate response actions for different circumstances depending upon the nature of the anomalous request. The two main issues that address in context of such response policies are that of policy matching, and policy administration. In this propose a novel Joint Threshold Administration Model (JTAM) that is based on the principle of separation of duty, present design details of JTAM which is based on a cryptographic threshold signature scheme, and show how JTAM prevents malicious modifications to policy objects from authorized

In this as a future enhancement present a high-level, informal overview of approach, and describe how implement the enforcer and the reference monitor. The first step that of determining the security sensitive operations to be protected, is manual. Typically, a design team considers security requirements for the server, and determines security-sensitive operations based upon these requirements. The design team typically considers a wide range of policies to be enforced by the server. Because security-sensitive operations are typically the granularity at which authorization policies are written first, identifying security-sensitive operations is a manual process, and plan to develop tool-support to assist with this task.

REFERENCES

[1] Contry Murray A. (2009) ,"The Threats from within Network Computing "

[2] Natan R.B. (2005) ,"Implementing Database Security and Auditing". Digital press.

[3] Ceri S. and Widom J.(1995) ,"Triggers and Rules for Advanced Database Processing"

[4] Koc C.K. (1994) , "High Speed RSA Implementation ". Technical Report tr.201, Version 2.0

[5] Chaabouni M. and Hanson E.M(1990), " A Predicate Matching Algorithm for Database Rule Systems", Proc. ACM SIGMOD , Vol 19 No. 2 pp . 271-280,

[6] Mogull R.(2006) ,"Top Five Steps To Prevent Data Loss and Information Leaks"