Protecting Database from Malicious Modifications Using JTAM

Raji V
Asst. Prof., Dept of CSE
SKP Engg., College,
Thiruvannamalai.

Ashokkumar P
Dept of CSE
SKP Engg., College
Thiruvannamalai

Abstract- 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. The 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 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 paper intend to report results on the overhead of the entire system on the transaction processing capabilities of the DBMS.

Keywords: *database administrator, intrusion detection.*

I. INTRODUCTION

Organizations have also come to realize that current attack techniques are more sophisticated, organized, and targeted than the broad-based hacking days of past. Often, it is 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 access control, authentication and encryption, are not of much help when it comes to preventing data theft from insiders. Monitoring database to detect potential intrusions, intrusion detection 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 exfiltration are not malicious for the underlying operating system or the network.

There are three main types of response actions, that we 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. With such different response options, the key issue to address is which response measure to take under a given situation. Note that it is not trivial to develop a response mechanism capable of automatically taking actions when abnormal database.

Related Work

Another approach toward addressing the problem of insider threats from malicious DBAs is to apply the principle of least privilege. The principle dictates that a user must be assigned only those privileges that are necessary to serve its legitimate purpose. This effectively means to restrict the privileges of the DBAs, and to create new roles for administration of response policy objects. Such approach is followed by Oracle Database using the concept of a protected schema for the administration of the database vault policies. Database vault is a mechanism introduced by Oracle Database to reduce the risk of insider threats by using policies that prevent the DBAs from accessing application data. A protected schema guards the schema against improper use of system privileges such as SELECT ANY TABLE, DROPANY, and so forth. Only the DVDSYS user and other database vault roles can have the privileges to modify objects in the DVSYS schema.

II. THE MODEL

This project has five modules. They are User privilege, Joint threshold Administration model, Policy Matching, Preparation of session key and Admin validation.

1. User Privilege

User privilege is nothing but the access authentication of the database table. The main issue in the administration of response policies is how to protect a policy from malicious modifications made by a DBA that has legitimate access rights to the policy object. Some of the users have minimum priority level they will access the database with certain level. Some of the peoples have maximum priority. So we have to give proper permissions to the users. To address this issue, we propose an administration model that is based on the well-known security principle of separation of duties (SoD).

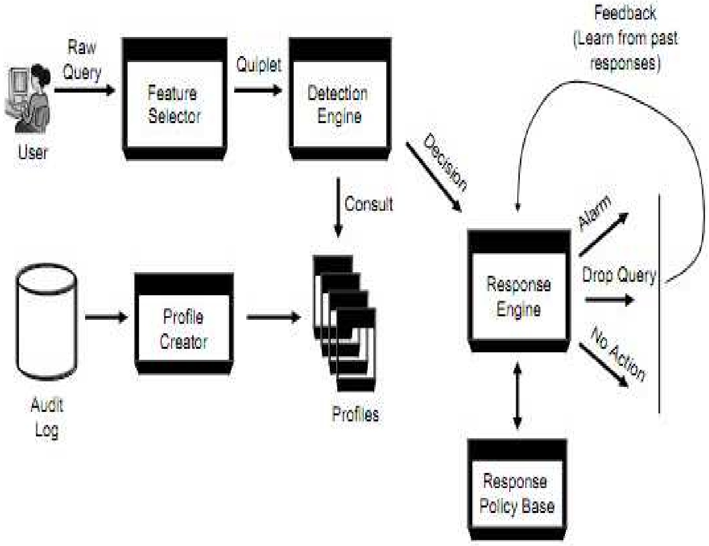

Figure:1 Architecture Diagram

2. Joint Thershold Administration Model

Joint administration model referred to as the JTAM. The threat scenario that we assume is that a DBA has all the privileges in the DBMS, and thus it is able to execute arbitrary SQL insert, update, and delete commands to make malicious modifications to the policies. Such actions are possible even if the policies are stored in the system catalogs. The key idea in JTAM is any modification made to a policy object will be invalid unless it has been authorized by at least k DBAs.

3. Policy Matching

In this section, algorithms for finding the set of policies matching an anomaly. The policies are stored in the system catalog tables. The policy matching algorithm is invoked when the response engine receives an anomaly detection assessment. Evaluating a predicate, the algorithm visits all the policy to the evaluated predicate. If the 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.

4. Preparation of Session Key

If the admin of a particular department wants to modify the values in the table means it will reflect the other entire 7 table. So the over all head of the relational database manager provide the key for the entire database. So no user can individually access or change the database. One of the key assumptions is that we do not assume the DBMS to be in possession of a secret key for verifying the integrity of policies. If the DBMS had possessed such key, it could simply create a HMAC of each policy using its secret key, and later use the same key to verify the integrity of the policy.

5. Admin Validation

Over all control of all database maintained by an administrator, like DBA. One user wants to change the consistency of the database means, admin checks the level of query, that will satisfies with the admin means he will allow the user with warning. Or else the control of the user will be deleted from the log.

III. SECURITY ISSUES OF DATABASE

Early research efforts focused on defining a proper security policy in the database security policy including user identification/authorization policy, access control policy, inference policy, accountability policy, audit policy and consistency policy. Some important principles were introduced in the security policy development to design a good database security policy; minimum vs. maximum principle, open vs. closed system principle, centralized vs. decentralized administration principle, granularity principle and access privilege principle.

REFERENCES

1. R. Mogull, "Top Five Steps to Prevent Data Loss and Information Leaks. Gartner Research (July 2006)," http://www.gartner.com,2010.
2. M. Nicolett and J. Wheatman, "Dam Technology Provides Monitoring and Analytics with Less Overhead. Gartner Research (Nov. 2007)," http://www.gartner.com, 2010.
3. R.B. Natan, Implementing Database Security and Auditing. Digital Press, 2005.
4. D. Brackney, T. Goan, A. Ott, and L. Martin, "The Cyber Enemy within ... Countering the Threat from Malicious Insiders," Proc.Ann. Computer Security Applications Conf. (ACSAC). pp. 346-347,2004.
5. Kamra A., E. Terzi, and E. Bertino, "Detecting Anomalous Access Patterns in Relational Databases," J. Very Large DataBases (VLDB), vol. 17, no. 5, pp. 1063-1077, 2008.
6. Kamra, A. E. Bertino, and R.V. Nehme, "Responding to Anomalous Database Requests," Secure Data Management, pp. 50-66, Springer, 2008.
7. Kamra A. and E. Bertino, "Design and Implementation of SAACS:A State-Aware Access Control System," Proc. Ann. ComputerSecurity Applications Conf. (ACSAC), 2009.
8. "Postgresql 8.3. The Postgresql Global Development Group,"http:// www. Postgresql .org/, July 2008. J. Widom and S. Ceri, Active Database Systems: Triggers and Rules for Advanced Database Processing. Morgan Kaufmann, 1995.
9. "Oracle Database Concepts 11g Release 1 (11.1)," http:// download.oracle.com/docs/cd/B28359_01/server.111/b28318/datadict.htm, July 2009.
10. Shoup V., "Practical Threshold Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), pp. 207-220, 2000.
11. Gennaro, R. T. Rabin, S. Jarecki, and H. Krawczyk, "Robust and Efficient Sharing of RSA Functions," J. Cryptology, vol. 20, no. 3, pp. 393-400, 2007.
12. Kincaid D. and W. Cheney, Numerical Analysis: Mathematics of Scientific Computing. Brooks Cole, 2001.
13. "Openpgp Message Format. rfc 4800," http://www.ietf.org/rfc/ rfc4880.txt, July 2009.
14. A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography. CRC Press, 2001.
15. C.K. Koc, "High-Speed RSA Implementation," Technical Report tr-201, Version 2.0, RSA Laboratories, 1994.
16. "Oracle Database Vault Administrator's Guide 11g Release 1 (11.1)," http://download.oracle.com/docs/cd/B28359_01/ server.111/b31222/toc.htm, Jan. 2009.
17. F. Fabret, F. Llirbat, J.A. Pereira, I. Rocquencourt, and D. Shasha, "Efficient Matching for Content-Based Publish/Subscribe Systems," technical report, INRIA, 2000.
18. M.K. Aguilera, R.E. Strom, D.C. Sturman, M. Astley, and T.D. Chandra, "Matching Events in a Content-Based Subscription System," Proc. Symp. Principles of Distributed Computing (PODC), pp. 53-61, 1999.
19. J.A. Pereira, F. Fabret, F. Llirbat, and D. Shasha, "Efficient Matching for Web-Based Publish/Subscribe Systems," Proc. Int'l Conf. Cooperative Information Systems (CooplS), pp. 162-173, 2000.

20. T.W. Yan and H. Garcı´a-Molina, “Index Structures for Selective Dissemination of Information under the Boolean Model,” ACM Trans. Database Systems, vol. 19, no. 2, pp. 332-364, 1994.
21. Campailla, A. S. Chaki, E. Clarke, S. Jha, and H. Veith, “Efficient Filtering in Publish-Subscribe Systems Using Binary Decision Diagrams,” Proc. Int’l Conf. Software Eng. (ICSE), pp. 443-452, 2001.
22. E.N. Hanson, M. Chaabouni, C.-H. Kim, and Y.-W. Wang, “A Predicate Matching Algorithm for Database Rule Systems,” Proc. ACM SIGMOD, vol. 19, no. 2, pp. 271-280, 1990