ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Survey on Different Advanced Database Security Policies against Masquerade Attacks

Amin F. Shaikh[1], Prof. Yagnik A. Rathod[2]

PG Student, Department of CE, SardarVallabhbhai Patel Institute of Technology, Vasad, Gujarat, India[1]

Assistant Professor, Department of CE, SardarVallabhbhai Patel Institute of Technology, Vasad, Gujarat, India[2]

ABSTRACT: Due to increasing the number of users in any system, it becomes very unmanageable task for ensuring the database security. There are number of techniques used for the same but still they compromised by some attacks like SQL injection attack, Insider threats, Outsider attacks and various unknown attacks. An Intrusion Detection System (IDS) is the technique used to detect this kind of attacks and malicious activity occurred in database. For any organization providing security by user id, password, database access rights etc. are not enough which can ensure against unauthorized data access, anomaly detection and so on. It is said that for any system the database is required to be more secure than any other. Traditional security mechanisms like firewall are no longer effective in today's environment because in web-based behavior, business partners and customers must have access to data including organization's employee. This kind of web applications connected to the Internet and accessing the back end databases, makes the DBMS more vulnerable to attacks. In this paper we discuss some advance security techniques for detecting the attack or unusual usage of sensitive data stored in the database repositories.

KEYWORDS: Database Security, IDS, Intrusion Detection, Data mining using IDS

I. INTRODUCTION

Data represent today are an important asset in any organization. Due to an increasing number of organizations that collect data, providing the secure environment for data access becomes distressing task. The data collected from various sources used for various purposes ranging from scientific research to demographic trend analysis and marketing purpose. Due to system integrations, organizations may also require for giving access to their data or even releasing such data to third parties which increases the number of the users and poses serious threats against the privacy of the sensitive data. By providing the basic security mechanisms, one cannot assure about the sensitive data to be secured, instead it is necessary for advance security policies to be implemented. Data security can be divided as secrecy, integrity and availability. Many of organizations employ DBMS as the main technology of data management in order to store and access their data. This Information is often considered as a valuable asset in the organizations. Hence, the data in the databases must be protected from unauthorized access and changes. Traditional database security mechanisms such as encryption, access control, and authentication are not sufficient for protecting of sensitive information against innovative security attacks. Analysing and monitoring the events occurring in database system for detecting signs of security threats, known as intrusion detection system (IDS). Intrusion detection systems (IDSs) in the database can be used for detecting attacks whenever traditional prevention mechanisms are infeasible or may be bypassed. In IDS audit data is analysed and judgment is done based on its normal behaviour, abnormal behaviour and the system is notified against the intrusion if it occurs [1]. An intrusion detection system (IDS) is growing popularity to provide another layer of defence against malicious (unauthorized) access of computer systems of a security policy and altering operators to an ongoing attack. IDS systems are capable to detect the known attacks as well as unknown attacks. Data mining techniques can be classified as misuse detection and anomaly detection [2]. A classification based approach known as misuse detection attempts to match observed activity to known intrusion patterns whereas anomaly detection tries to detect behaviour that does not belong to normal behaviour. IDSs also works on the basis of audit data source which may be network based or host based. Variety of audit data sources is required for successful detection of different types of attacks. Building IDS is a very complex task and need an array of diverse components and features including

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

centralized view of data, data transformation capabilities, data mining methods, real-time detection and alert infrastructure, data analysis and system availability [3].

II. RELATED WORK

Database security define as to comprise a set of measures, policies, and mechanisms to provide secrecy, integrity and availability of data and to battle possible attacks on the system from insider and outsiders, both malicious and accidental [4]. In other words, Data security can be defined as protecting information against unauthorized disclosure, alteration or destruction using hardware or software techniques [5]. One can assure security in DBMS by identifying the threats and choosing the proper rules and policies which refer to what the actual system behavior [6] and mechanisms which refer to how the security system should achieve the security goals [7].

Database management systems have three major security issues of concern: confidentiality, integrity and availability. Confidentiality refers to information disclosure only to those users authorized to access it. The improper release of information caused by reading data from intentional or unintentional access either observed or inferred is considered a breach of data confidentiality. Integrity is the second security issue of database management systems. There are several areas of database integrity: physical database integrity, logical database integrity and data element integrity. Physical database integrity protection maintains data integrity through physical problems such as power failures and fires. Logical data integrity protection refers to the assurance that information is modified only by users entitled to do so. Maintaining data element integrity involves data accuracy and correctness. The third issue is availability. This issue involves maintaining access to the database and all the data within the user's authorized domain. A denial-of service attack involves actions that prevent users from accessing or using the database. Threats to any of these categories are a breach of security and must be prevented. Any breach in security to these databases can affect the reputation of the organization, loss of customers' confidence and might even result in lawsuits.

III.ADVANCE TECHNIQUES FOR IDS

A. Intrusion detection in role administrated database: transaction- based approach [8]

In this paper, Anomaly detection approach that summarizes the raw transactional SQL queries into compact data structure called hexplet, which can model normal database access behaviour (abstract the user's role profile) and recognize impostors specifically tailored for role–based access control (RBAC) database system. This hexplet allows us to preserve the correlation among SQL statements in the same transaction by exploiting the information in the transaction-log entry. The target is to improve detection accuracy, specially the detection of those intruders inside the organization who behave strange behaviour. The method they have used to classify the user as a legitimate or masquerade by Naive Bayes Classifier (NBC) as a simple technique for evaluating the legitimacy of transaction.
They improved the representation of SQL commands to also include information about the whole transaction. The ID system they have discussed is able to build a profile for each role and is able to conclude role intruders, that is, individuals that while holding a definite role diverge from the normal activities of that role. With respect to ID, using roles means that the number of profiles to form and maintain is much smaller than those one would need when considering individual users. This implies that an ID solution, based on RBAC, could be easily deployed in practice.
To improve the performance of this method and reduce the false positive rate to be 0, they have performed a very simple check before applying our detection method. We can check the new transaction hexplet against stored hexplets for the role of the user issued the transaction. If it matches any of existing hexplet for his role then the transaction won't be anomalous otherwise we apply our detection method on the transaction to validate it. This track helps in many situations like when a role made a regular transaction rarely, so, if we applied our detection method directly, a false positive will appear in this case.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

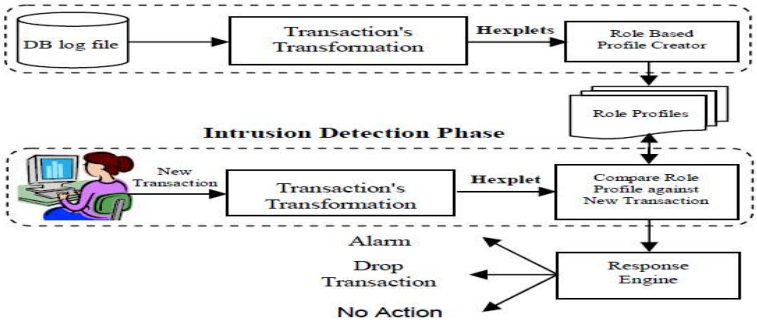

Fig 1: Database IDS using hexplet ID mechanism. [8]

As described in fig. 1, this machine learning system capable of extracting valuable information from the log files regarding the access patterns of queries in the same transaction. The use of roles that are employed for training a classifier makes this system practical even for databases with large user population. As compared to query-based approaches, this system will certainly enhance the false negative rate as it has deliberated the correlation among queries of a transaction.Response engine shown in fig. 1, used to make a decision based on the result of the comparison made in the above phase, and will decide whether to allow the query for being processed or to alert the system if any of the intrusion detected.

B. Database intrusion detection by transaction signature [9]

In this paper they have discussed on security policies for transactions permitted with DBMS. The approach is designed to mine audit log of legitimate transaction performed with database and generate signature for legal transactions as per security policy. The transactions not compliant to signature of valid transaction are identifies as malicious transaction.

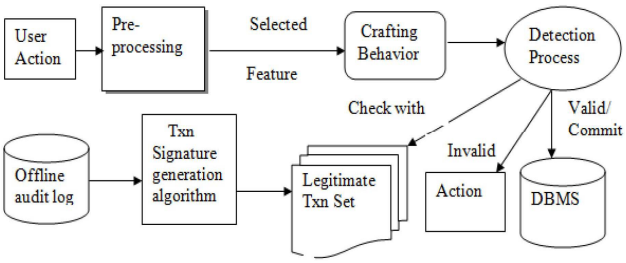

Fig 2: IDS by transaction signature [9]

As described in fig. 2, the first phase is known as learning phase. Normal or legitimate behaviour is understood in this phase. We have records in audit log of DBMS which contains user'snormal or say legitimate action as per security policy of system. All historical transaction with database is accessed to understand behaviour of legitimate transactions. In the second phase known as signature generation, in which the legitimate signature is generated based on the user's action which is then be used for the next module. The third phase known as response phase, in which the decision is made based on whether user's action is legitimate or not. The output of the previous module - signature generation algorithm, will be compared with signature derived from historical data. Based on this comparison this module will decide what action should be taken. The query will be allowed if the current signature of the current transaction match with the legitimate transaction which we had defined earlier, or else the system will fet alert or the query will be aborted.

The discussed intrusion detection mechanism that can provide an additional security layer to the database to detect the database intrusion and it can be considered as generic approach for any database application to detect the malicious activities.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

C. System architecture for SQL injection and insider misuse detection system for DBMS [10]

This paper defines the attacks related to SQL injection refers, a class of code-injection attacks in which data provided by the user is included in the SQL query in such a way that part of the user's input is treated as SQL code. It is a trick to inject SQL query or command as an input possibly via the web pages. They occur when data provided by user is not properly validated and is included directly in a SQL query. In their proposed system, they have combined anomaly and misuse detection methods to give the database server a way to mitigate the SQL injection and insider misuse attacks.

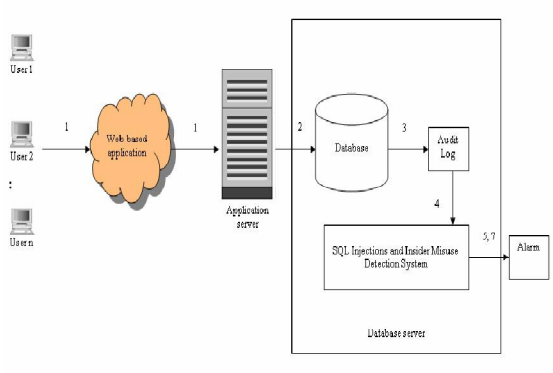

Fig 3: A SQL injection and misuse IDS. [10]

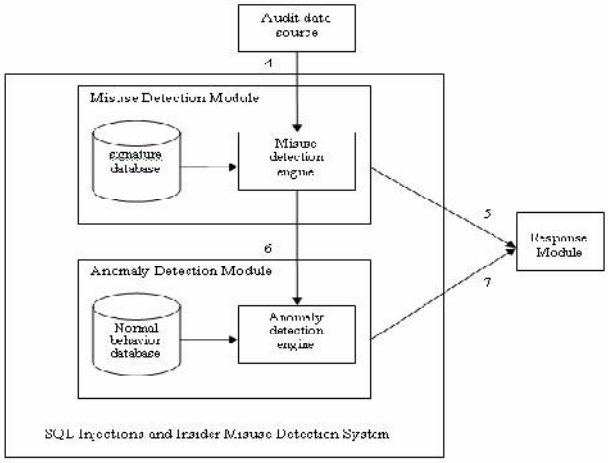

Fig 4: A SQL injection and misuse IDS. [10]

The basic architecture of the system is depicted in fig. 3. In the first step, user requests the application server through a web-based application that request may or may not be legitimate request. Then after the application server deploys the SQL query statements and issues to the database server. Database session is traced while any user logs into the system. The SQL statements which are received earlier are channelled to the misuse detection module in which the received SQL statements are matched with the set of SQL injection's signatures.

Here an intrusion is occurred if the SQL statement matches with the SQL injection signatures. The intrusion is then channelled to the Respond Module for the appropriate action(s) to be taken. As described in fig. 4, In Misuse Detection Module no intrusion is detected then the SQL statements are channelled to the Anomaly Detection Module to check whether the SQL statements are different from the normal database access behaviour.If the SQL statements are different from the normal database access, an internal misuse is concluded as has occurred and this misuse will be channelled to the Response Module for the appropriate action(s) to be taken. The appropriate decision can be made include the alerting of administrator by sounding the alarm.

D. A hybrid approach for database intrusion detection at transaction and inter-transaction levels [11]

In this paper authors proposed a type of intrusion detection system for detecting attacks in both database transaction level and inter-transaction level (user task level). The basic architecture of the proposed system is depicted in the fig. 5.They have used detection method at transaction level, which is based on describing the expected transactions within the database applications. Then at inter-transaction level, second detection method that is based on anomaly detection and uses data mining to find temporal patterns and rules. The advantage of this system compared to the previous database intrusion detection systems is that it can detect malicious behaviours in both transaction and inter-transaction levels using a hybrid approach, including specification-based detection and anomaly detection. In order to evaluate the accuracy of the proposed system, some experiments have been done. The experimental evaluation results show high accuracy and effectiveness of the system.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

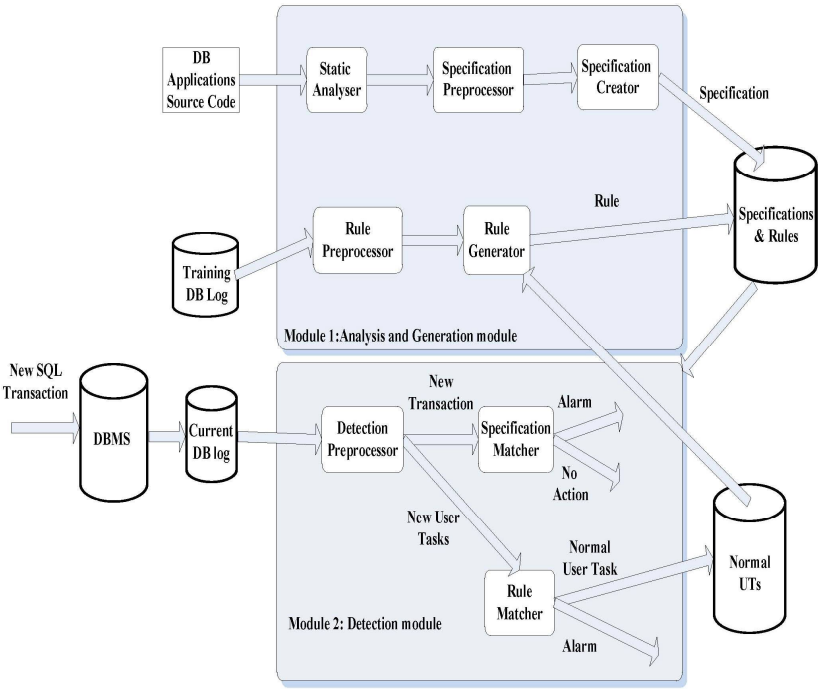

Fig 5: Hybrid Approach for DADS at Transaction and Inter-transaction Levels [11]

Static Analyser component shown in fig. analyses the source code of database applications in the organization and places extracted information from identifying transactions into a file named Specification, the next phase called Extracting Transaction Information extracts the information related to SQL queries. The next step is specification Creator component creates a state machine specification for each expected transaction, which is based on the information derived from the SQL queries within the intended transaction.
Inter-transaction Temporal Rules Generating phase in which, Rule Generator component is used for discovering the temporal relation patterns and rules among the expected transactions. For this purpose, the component uses vectors received from the Rule. Pre-processor component that contain information about the existing transactions in the identified user tasks The Detection module identifies the malicious transactions and the abnormal user tasks based on the existing transaction specifications and existing inter-transaction rules respectively. For this purpose, the Detection module examines the SQL queries issued by database applications in the form of transactions and user tasks stored in the current database log file. The main advantage of proposed system is the use of a hybrid method, including specification-based detection and anomaly detection.

E. Hybrid approach for database intrusion detection with reactive policies [12]

This paper introduces the concept of reactive policies and describes an approach for finding the intrusive activity using Apriori algorithm. Reactive policies are nothing but the action rules which defines to be taken if any intrusion occurs. Response is generated for the users who performed intrusive activity based on the severity of an intrusion. In this paper they have used Misuse and Anomaly detection for IDS. Misuse detection also known as signature based detection which is used for known attacks while Anomaly detection is based of detecting unknown attacks. Due to known patterns of attacks already available in Misuse detection, its false alarm is less but the disadvantage of this method is that it can only detect known attacks. While anomaly detection technique can detect unknown attacks but its drawback is that it has high false alarm rate. As shown in fig. 6, the first step in designing DIDS is to collect the logs of user activity from audit trail. For better intrusion detection it is required that the user activity collected and processed properly. In preprocess logs are collected and arranged in proper format which consists of attributes of user and its corresponding activity. Each activity

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

defines an operation ID and its status ID.For market basket applications, Data mining plays an important role to analyze market trends.

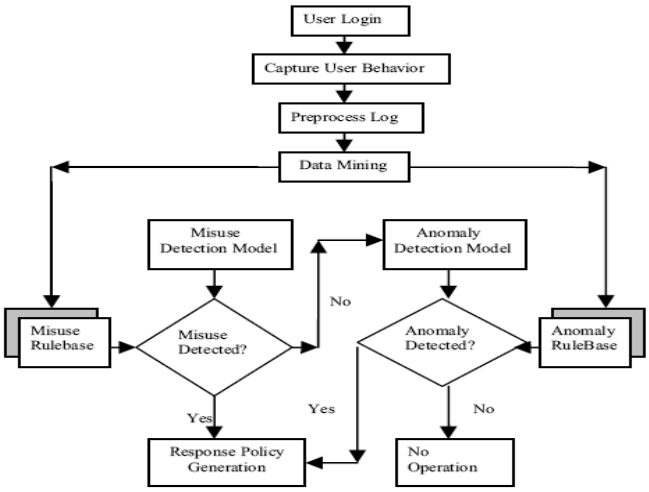

Fig 6: HIDIDS Architecture [12]

Here, the threshold level is defined by observing large datasets in which the frequent items occurs, and if that threshold value crosses for certain associations, a strong rule is generated. This rule in our case gives an exact strategy for intruders. Apriori algorithm is the very popular technique in association rule mining, which gives us the association patterns that are useful for detecting intrusions. In this paper data mining technique is used to find out associations in user activity. Several attributes of user activity are collected and associations are observed. Then after for every abnormal behavior a reactive policy is applied. Then test phase decides intrusion or normal behavior by mining audit log. It captures both the normal as well as abnormal activities of the database user and then later it will be compared with the legitimate or say accepted patterns which we had derived during our training phase. Due to its hybrid behavior it is able to detect known as well as unknown attacks and assures the secure access of sensitive data in database.

IV. CONCLUSION

For securing the database against intrusion and malicious transactions, there are numbers of methods implemented, but still there is possibility of masquerade attacks which may harm the current system and leads the system in dangerous state. So it becomes necessary for the improvement in the detecting intrusive activity and threats which can assure the secure access of sensitive data stored in database only for the valid authorized users in any organization. Here we had discussed some advance techniques known as IDS for database which assures the secrecy, confidentiality i.e. by disclosing the data only to secured environment.

REFERENCES

1. Wu, G., & Huang, Y. Design of a new Intrusion detection system based on database. In 2009 International Conference on Signal Processing Systems IEEE, (pp. 814-817), 2009
2. Noel, S., Wijesekera, D., &Youman, C. (2002). Modern intrusion detection, data mining, and degrees of attack guilt. In Applications of data mining in computer security, Springer US. pp. 1-31, 2002
3. Lee, W., &Stolfo, S. J. (2000). A framework for constructing features and models for intrusion detection systems. ACM transactions on Information and system security (TiSSEC), 3(4), 227-261, 2000
4. Asmawi, Aziah, Zailani Mohamed Sidek, and ShukorAbdRazak. "System architecture for SQL injection and insider misuse detection system for DBMS." In Information Technology, 2008. ITSim 2008. International Symposium on,. IEEE,vol. 4, pp. 1-6 2008.
5. Asmawi, Aziah, Zailani Mohamed Sidek, and ShukorAbdRazak. "System architecture for SQL injection and insider misuse detection system for DBMS." In Information Technology, 2008. ITSim 2008. International Symposium on, IEEE, vol. 4, pp. 1-6, 2008.
6. Olson, Ingrid M., and Marshall D. Abrams. "Computer access control policy choices." Computers & Security 9, no. 8 699-714,1990
7. Bell, D. Elliott. "_,"Lattices, Policies, and Implementations,"." In 13th National Computer Security Conference, pp. 165-171. 1990.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

8. Darwish, Saad M., Shawkat K. Guirguis, and Mahmoud M. Ghozlan. "Intrusion detection in role administrated database: Transaction-based approach." In Computer Engineering & Systems (ICCES), 2013 8th International Conference on, IEEE,pp. 73-79. 2013.
9. Rathod, Yagnik A., M. B. Chaudhari, and G. B. Jethava. "Database intrusion detection by transaction signature." In Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, IEEE, pp. 1-5, 2012.
10. Asmawi, Aziah, Zailani Mohamed Sidek, and ShukorAbdRazak. "System architecture for SQL injection and insider misuse detection system for DBMS." In Information Technology, 2008. ITSim 2008. International Symposium on, vol. 4, IEEE, pp. 1-6, 2008.
11. Doroudian, M., &Shahriari, H. R. Database intrusion detection system for detecting malicious behaviours in transaction and inter-transaction levels.In Telecommunications (IST), 2014 7th International Symposium on,).IEEE,pp. 809-814, 2014
12. Shedge, Rajashree, and LataRagha. "Hybrid Approach for Database Intrusion Detection with Reactive Policies." In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, IEEE pp. 724-729. 2012.

BIOGRAPHY

Amin F. Shaikh is a PG student in Department of Computer Engineering at SardarVallabhbhai Patel Institute of Technology, Vasad, Gujarat, India. He received Bachelor of Engineering in CSE (BE CSE) degree in 2014 from GTU, Gujarat, India. His research interest is Database security.

Yagnik A. Rathod is an Asst. Professor in the computer Engineering Department, SardarVallabhbhaiPatel Institute of Technology, Vasad, Gujarat, India.He received Bachelor degree in Computer Engineering in 2003 from D.D.I.T.,Nadiad and degree of M.Tech. in Computer Engineering in 2012 from Government College of Engineering, Gandhinagar, Gujarat, India. His area of interest is Database Management System.