Protecting Database from Malicious Transactions by Intrusion Detection Using TAP and RBLM

Surya Pratap Singh, Upendra Nath Tripathi, Manish Mishra
Department of Computer Science
Department of Electronics
Deen Dayal Upadhyay Gorakhpur University, Gorakhpur (U.P.) – 273009

Abstract

The database uses is growing at a very high rate in recent years so the need of securing the database from various types of attacks becomes more important for all types of organizations. The malicious attacks are very frequent these days they cause loss of sensitive data and information. The existing security procedures and countermeasures are not fully able to protect the databases from various malicious attacks due to variety of reasons. The most important reason is that the attacker on the database may be an insider. The main objective of this paper is to provide an intrusion detection system that is able to detect the insider’s misuse over the database and provide full protection to the database and be extensible and reliable and adaptive to the flow of network traffic and to have a low cost of maintenance. This paper provides an overview of malicious transactions in databases and provides mechanism to secure it using intrusion detection. This paper also proposes two intrusion detection mechanisms Role Based Log Monitor and Transaction Verification Protocol.

Keywords – Database System, Malicious transactions, IDS (Intrusion Detection System), TAP, RBLM.

1. Introduction

The use of Internet and computer increases rapidly in past few decades, all organizations are now using the computerised way to do the business and communicate with the user and customers. All these applications need some mechanism to store data related to, so the database is used heavily in all these places. In recent years various types of database attacks are done, as a result there is loss of confidential data and computations. So the database security is very important now these days.

There are various aspects in database security such as security at the database layer and security at application layer. The application level security can be implemented through complex access control policies, but if anyone has the direct access to the database he/she can bypass these access control policies and do the malicious actions [9]. In this way additive to the DBA (Database Administrator) anyone who fiend the database login and password used in the application can directly modify the database. Thus, even if all the security policies have been enforced to ensure security in the database we need some mechanism to detect and protect the database from malicious transactions. To support this type of detection and protection we need database intrusion detection system wherein malicious transactions may be detected while system still having the application level security. [10] Now day’s application based on database system is common, often storing critical data that should not compromised in anyway. Such types of applications are built on multi-layer of security: at the top level the application software, typically running on a web server, at the next level is the database system which stores the data and bellow the database system or the operating system and storage system layer. [11] Security of application requires actions at each layer. In this paper we focus on the database layer where the data is reside and we provide protection mechanism to these data.

The application level security is implemented through various complex access control mechanisms where if someone gains access to the user name and password then he/she can frequently modify the contents stored in the databases this is because the user name and password information are stored in the database in simple text form and can be accessed by the system administrator so we need some type of security mechanism by which we can disallow malicious update /transactions in the database.

2. Review of Literature

H. Gunes - [1] performed a feature relevance analysis on KDD 99 training set, which is widely used by machine learning researchers. Feature relevance is expressed in
3. Threats to databases

Threats to databases result in the loss or degradation of some or all of the following commonly accepted security goals. [3]

- **Loss of integrity** – Database integrity refers to the requirement that information be protected from improper modification. Modification of data includes creation, insertion, modification, changing the status of data and deletion.
- **Loss of availability** – Database availability refers to making objects available to a human user or a program to which they have a legitimate right.
- **Loss of confidentiality** – Database confidentiality refers to the protection of data from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from violation of the data privacy act of the jeopardization of national security.

In a way to securing the data into the databases we can also classify security and integrity threats in the categories of accidental or intentional or malicious.

3.1 Accidental security and Integrity Threats

- A user can get access to a portion of the database not normally accessible to the user due to system error or an error on the part of another user.
- Failures of various forms during normal operations.
- Concurrent usage anomalies.
- System errors.
- Improper authorization.
- Hardware failures.

3.2 Malicious or intentional security and Integrity Threats

- A computer system operator or system programmer can intentionally bypass the normal security and integrity mechanism, alter or destroy the data in the databases or make unauthorized copies of sensitive data.
- Authorized users could pass on sensitive information under duress or for personal gain.
- An unauthorized user can get access to a secure terminal or the password of an authorized user and compromise the database.
- An unauthorized person could get access to the computer system, physically or by using a communications channel, and compromise the database.

4. Defence Mechanisms

Four levels of defence are generally recognized for database security: human factors, physical security, administrative controls, and the security and integrity mechanism built into the operating system and the DBMS. [4]

4.1 Security Policies
To prevent the dissemination of sensitive information from the database to unauthorized users and thence to outside competitive or hostile agents, an organization must establish effective security policies. Database security mechanisms are the functions used to enforce database security policies. These functions could be implemented by a combination of one or more of the following –

- Administrative control procedures
- Hardware functions
- Software functions
- Firmware functions

4.2 Authorization

Authorization is the culmination of the administrative policies of the organization, expressed as a set of rules that can be used to determine which user has what type of access of which portion of the database.[5] The person who is in charge of specifying the authorization is usually called the authority. The authority can be distinct from the DBA and usually is the person who owns the data. The authorization is usually maintained in the form of a table called an access matrix.

<table>
<thead>
<tr>
<th>SUBJECTS/OBJECTS</th>
<th>EMPLOYEE</th>
<th>READ</th>
<th>MED_HISTOR RY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>Read except Salary</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Secretaries</td>
<td>Read except Salary</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Chairperson</td>
<td>Read except Salary</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Physicatian</td>
<td>Read except Salary</td>
<td>Read</td>
<td>Read</td>
</tr>
<tr>
<td>Director of personal</td>
<td>Read</td>
<td>Read</td>
<td>Reademployee_name, date</td>
</tr>
</tbody>
</table>

Fig 1 Access matrix

The access allowed to a user could be for data manipulation or control. The operations are – Read, insert, delete, update, add, drop, alter, and propagate access control.

4.3 Identification and Authentication

the enforcement of the security policies in the database system requires that the system knows the identity of the user making the requests.[6] This in turn requires that before making any request, the user has to identify him/her to the system and authenticate the identification to conform that the user is in fact the correct person. This can be achieved by the following ways –

- Something known only by the user
- Something in the user’s possession
- Some characteristic of the user

4.4 Views / subschemas in Security Enforcement

the mechanism of views is an important authorization mechanism its own right. For example – if the owner A of a relation R wants another account B to be able to retrieve only some fields of R, then A can create a view V of R that includes only those attributes and then grant SELECT on V to B. The same applies to limiting B to retrieving only certain tuples of R.

4.4 Integrity

Security constraints guard against accidental or malicious tempering with data, whereas integrity constraints ensure that any properly authorized access, alteration, deletion or insertion of the data in the database does not change the consistency and validity of the data. This requires that there is a need for guarding against invalid database operations.

Database integrity involves the correctness of data. This correctness has to be preserved in the presence of concurrent operations, errors in the user’s operations and application programs, and failures in hardware and software.

In traditional systems, application programs were responsible for the validation of data and maintaining the consistency of the data used by the program.[7] However, in a DBMS environment, depending on the application programs to perform these checks has the following drawbacks.

- Each application program must have correct validation and consistency check routines.
- Each application program must be aware of the semantics of the complete database to enforce the correct consistency checks.
- There will be considerable duplication of efforts.
- Integrity constraints are hard to understand when they are buried in the code of application programs.
- No consistency or validity checks are possible for direct database manipulation using a query language.

5. Problems in existing system
The problem of intrusion detection remains very crucial in past few years many researchers of database and network security provided different approaches to counterfeite the situation, but none of the approach is able to fully secure the database. Every approaches presented by the researchers are based on preventing the database form attackers who are outsiders or not a legal user but the intruder can be a legal user but somehow intentionally/unintentionally gain access to those portion of the database that he is not have right. There is strong probability of these types of attacks and there is a lot of security aspect to cover.

Another problem with the existing approach of intrusion detection system is that most of systems provide all or nothing method of user access, if somehow the user logs in to the system then user can perform malicious transection and harm to the database so there is need to design multilevel security.

6. Proposed methodology

to secure the database from malicious transection various researchers and practitioners proposed there strategy but none of these strategy is able to fully secure the database form these malicious transection. In this paper we propose intrusion detection mechanism to protect the database from these problems

6.1 Intrusion detection by Role Based Log Monitor (RBLM)

In this method we propose role based access control to provide application level security every user is assigned to a predefined role and when the user trying to log in to the system by valid user name and password he/she is associated with these roles. In addition, we propose a role based log monitor which stores allowed log pattern to the database users.

Fig 2: Architecture of intrusion detection by RBLM

Fig 2 explains the architecture of the intrusion detection system by RBLM in this approach user first log in to the web server using Role based Authentication procedure by providing user name and password, after login the user can queries the database In this process the RBLM continuously monitor and match the queries provided by the user to that stored in the database and if any deviation is found to the stored pattern the system identifies it as malicious transection and triggers an alarm.

6.2. Intrusion detection using transection authentication protocol (TAP)

in this approach we propose TAP (transection authentication protocol) by which the multilevel transection security can be provided, under this scheme the login into the system is done by traditional username and password authentication mechanism, the database normal processing can be done in normal way but when the user tries to perform some complex transection then TAP authenticate the user privilege. To achieve this we propose two ways to do it : in first approach a secure online transection authentication code is generated for each session by TAP. In second approach we propose unsupervised biometric verification before committing the transection where we create an abstraction by which the biometric verification process is hidden to the user. If any deviation is found in this process the system treats it as intrusion and triggers alarm.

7. Conclusion

the database security is very crucial in today’s environment, the malicious transactions can compromise the database security as if any intruder gain access to the database then he/she can case enormous harm to the database contents so there it an extensive need for intrusion detection system by which any attempt of intrusion can be identified and the database is protected from these malicious transection, various approaches to detect intrusion in the database are proposed by different researchers but none of these approaches are fully able to detect intrusion. This paper proposed two approaches RBLM and TAP by which the intrusion can be detected easily even if some legal user tries to perform malicious transactions in database.

8. References

11 WG 11.5 Conference on integrity and internal control in information system, pp. 159-178, 1999.

Author’s Profile

Mr. Surya Pratap Singh is pursuing PhD. In the department of computer science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. Area of research interest is Database Security, Networking. Mr. Surya Pratap Singh has published 05 papers in different national and international conferences/Journals.

Dr. Manish Mishra is Assistant professor in Department of Electronics DDU Gorakhpur University, Gorakhpur (U.P. India). He has 13 years of teaching and research experience. He has published 45 papers in various National and International Journals/conferences. His area of research interest is Computer Technology, fast processor design.

Dr. Upendra Nath Tripathi is Assistant professor in Department of computer science DDU Gorakhpur University, Gorakhpur (U.P. India). He has 13 years of teaching and research experience. He has published 40 papers in various National and International Journals/conferences. His area of research interest is database systems, networking.