International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 2, February-2016, Impact Factor: 1.544

A review on Security methods and threats in Database Management System

Meenakshi

ABSTRACT

At the present time in technical world a Database security has turn out to be a central issue. The needless information introduction and alteration data while ensuring the accessibility of the desirable services are the main objectives of database security. Numerous of security methods have been produced for shielding the databases. On different security aspects of database numerous security models have been developed. All of these security methods are helpful only when the DBMS is designed and developing for protecting the database. Presently the expansion of web application with database at its backend Secure DBMS is more important than only a Secure Database. In this paper on the Security Methods, Threats in DBMS using brief study done in the field of secure databases.

Keywords; threats, security methods, DBMS

1. INTRODUCTION

In present era securing database is a required feature. Individually every day we make use of database innocently when we surf on internet. The data we obtain on the web page is the result of query accomplished by the webpage to the database by which it is connected. That's why indirectly we are connected to different databases through the webpage. The web pages are unlocked for any unspecified person in the world. Data in the database is the mainly precious asset which is the source of information. So this information cannot be exposed for anyone.

2. PROTECTED DATABASE

There are lots of ways developed of securing the database. All these depend on different aspects of protecting the database. Different aspects with conventional approaches from different researchers study are summarized below:

P**rivacy**
Protection of data in opposition to unauthorized disclosure can be achieved using access control method. Encryption techniques are applied to data while storing on secondary storage or transmitted on a Network.

Veracity
Prevention of unauthorized and inappropriate data alteration and is achieved in combination of access control method by semantic integrity constraints.

Accessibility
Prevention and recovery from software and hardware errors and from malicious data access denials making the database system inaccessible. The data that are available on the Web can be motorized by the use of techniques protecting against denial-of-service(doS) attacks and such as the ones based on machine learning techniques.

Different Aspects
Latest approaches of protecting database are illustrated in [2]. All of these approaches are related to CIA. In these approaches the author proposes that it can be implemented with the help of below listed appropriate techniques[4]:

1. **Verification of Users**
2. **Access control to things and confirmation of authorized applications**
3. **Secure preliminary configuration**

4. **Auditing**
5. **Backup and recovery strategies**

3. THREATS IN DATABASE MANAGEMENT SYSTEM (DBMS)

Aziah Asmawi in [5] defined threat in database by some set of policies, procedures and methods to give availability, safety and integrity of data and to struggle probable attacks from outsiders as well as insiders on the system, both unintentional and malicious.

1 **Access through login page**: It is the easiest technique. In this where users are authenticated by using password it bypasses the login forms. This type of method can be completed by the attackers through: 'having' clause, 'or' condition and several queries.

2 Access through URL: This technique is used by attackers through: manipulating the query string in URL and using the SELECT' and UNION statements.
Further Ravi Sandhu [1] has described in his paper that threat to the database can be internal or external.

3 People: In this point the different people are concerned in DBMS. They can be a government authority , visitors, hackers, organized criminals, spies, an employee or a person-in charge, consultants, contractors, terrorists and social engineers may unintentionally exact damage on any of the database

4 Malicious Code : It refers to s/w code , in which most cases are purposely written to harm one or more of the database environment mechanism. These are boot sector worms, viruses, denial-of-service flood, bots, root kits, spoofing code Trojan horses and bots,
E-mail spamming, macro code.

5 Natural disaster: Calamities caused by nature can destroy any or the complete database environment components.

4. SECURITY METHODS IN DATABASE MANAGEMENT SYSTEM

In this we are discussing about few security methods in DBMS. Security methods in DBMS focus only on access control or maintaining the confidentiality of the database. However in the present state the unauthorized user operational on a web page which is associated through internet connection has right to use the database, as all the queries sent by the user is transformed to SQL query in that database. The user can send malicious query and modify or verify the transactions[3] of the database without touching the performance of the database. But in the present state the security method of database can focus on role base access control and avoid attacks due to network. In this discussion on the same has been done.

5 SECURING DATABASE BASED ON ACCESS CONTROL:

In this we have discussed the database security based on access control. By Guoliang Zou, Jing Wang, Dongmei Huang [6] has proposed the role based access control method. Author Ravi Sandhu has created a variety of security approaches [1] where he has measured that access control policies in early days were based on the development of two different classes of models, the discretionary access control policy and on the required access control policy and procedure. Based on these models of early days [7] have proposed two statements:

1 The access control models for databases can be described in terms of the logical data mode; was the first statement; hence authorizations for a relational database should be determined in terms of relational model such as relations, relation attributes, keys and tuples etc.

2 The second statement is that for databases, in succession to name-based access control, where the secure and sheltered items are categorized by giving their names

In addition the access control policies of an OODBMS are defined in [8]. In this point the author has discussed about two proposed security models for OODBMS. They are given below as:

1 **Sorion Security Model**

2 **Jajodia-Dogan Security[9] Model:**
By using the encapsulation characteristic of object oriented database [6] has proposed a security model for OOBBMS that control access. Hereafter by the access control policies and process the privacy of the database can be supported. Hereafter, Due to the accessibility of company's whole information on the web page which is connected via Internet to its database, the whole data of that company is obtainable using the SQL injection[10].

The second security issue of DBMS has a range of fields of database integrity as described in [5]:

Physical database integrity protection(PDIP): It manages data integrity through physical obstacles such as fires and power failures.

Logical data integrity protection(LDIP): It refers to the assertion that information is can be changed only by users.

Data element integrity protection: It involves data effectiveness and data regularity.

CONCLUSION

In this paper we have studied the threats and security methods of database management system. As a result we can say that though extraordinary work has been done in this field. The risk to database has increased with the discovery of internet technology. Numerous intrusion detection systems for the database have devised. Still researchers are doing more since there are vulnerabilities in internet connection and website.

REFERENCES

[1]. Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE, "Database Security—Concepts, Approaches and Challenges" in IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005
[2]. Andriy Furmanyuk , Mykola Karpinskyy, Bohdan Borowik, "Modern Approaches to the Database Protection" in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany
[3]. Marco Vieira, Henrique Madeira , "Detection of Malicious Transactions in DBMS", 11th Pacific Rim International Symposium on Dependable Computing
[4]. Hassn A. Afyuoni, A Book, "Database security and auditing "
[5]. Aziah Asmawi , "System Architecture for SQL Injection and Insider Misuse Detection System for DBMS", my -1-4244-2328 6/08/$25.00 © 2008 IEEE
[6]. Guoliang Zou, Jing Wang, Dongmei Huang, LiangJun Jiang, "Model Design of Role-Based Access Control and Methods of Data Security", 2010 International Conference on Web Information Systems and Mining.
[7]. E.B. Fernandez, R.C. Summers and C.Wood, Database Security and Integrity. Addison-Wesley, Feb. 1981.
[8]. Premchand B. Ambhore, B.B.Meshram,V.B.Waghmare, "A IMPLEMENTATION OF OBJECT ORIENTED DATABASE SECURITY" , Fifth International Conference on Software Engineering Research, Management and Applications.
[9]. Yu Chen and Wesley W. Chu, "Protection of Database Security via Collaborative Inference Detection ", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 20, NO. 8, AUGUST 2008
[10]. http://www.esecurityplanet.com/hackers/how-to-prevent-sql-injection-attacks.html