www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Vandana Publications
IJEMR

Volume-7, Issue-3, May-June 2017
International Journal of Engineering and Management Research
Page Number: 269-272

A Review on Database Security

Shelly[1], Gurleen Kaur[2]
[1]Assistant Professor (CSE), Rayat-Bahra University, Mohali, INDIA
[2]Student of M. Tech (CSE), Rayat-Bahra University, Mohali, INDIA

ABSTRACT

Protecting data is at heart of many secure systems and many users depend on a database management system to manage the protection. This paper is all about the security of database management systems, as an example of how application security can be designed and implemented for specific task. There is substantial current interest in a DBMS Security because databases are newer than the programming and operating systems. Databases are essential to many business and government organizations, to make the retrieval and maintenance of data easy and efficient it is stored in a database. Database organization and contents are considered valuable corporate assets that must be carefully protected because databases are a favorite target for attackers. The basic security requirements of database system are not unlike those of other computing system. The basic problems are access control, exclusion of specious data, authentication of users and reliability. In this paper the challenges and threats in database security are identified.

Keywords--- Attack, Database Security, Integrity, Threat

I. INTRODUCTION

Protecting data is the heart of many secure systems and many users depend on a database management system to manage the protection. Databases are essential to many business and government organizations, holding data that re-engineered to make them more effective and more tunes with new and revised goals [1]. Database security is difficult operation that any organization should enhance in order to run its activities smoothly. The various threats pose a challenge to the organization in terms of integrity of the data and access. The threats can result from either by an outside illegal program action or by an outside force such as fire or a power failure [1]. Most of the database contains sensitive data for users which can be unprotected to hacking and misuse [3].Therefore, firms have greater control and check on their database to maintain the integrity of the information and ensure that their systems are monitored closely to avoid deliberate violations by intruders.

II. THREATS OF DATABASE SECURITY

Database security issues have been more complex due to widespread use. Database are a firm main resource and therefore, policies and procedure must be put into place to safeguard its security and the integrity of the data it by contains. Besides, access to the database has been become more widespread due to the internet and intranets therefore, increasing the risks of unauthorized access. The objective of database security is to protect database from accident or intentional los. These threats pose a risk on the integrity of the data and its reliability. Database security allows a refuses users from performing actions on the database. There are different threats to the database systems. Such as Excessive Privilege Abuse when users are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose [3]. Another threat is a weak audit trial.

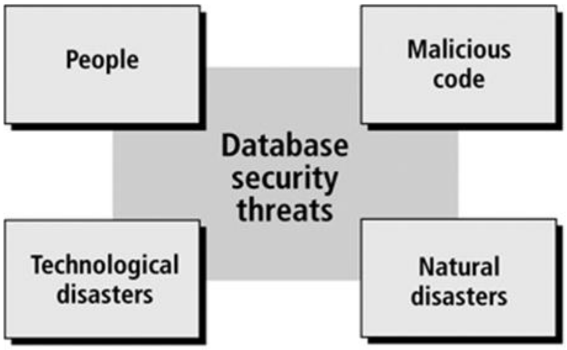

Figure 1: Threats of database security [3]

This is due to weakness in organizational internal system. This is due to weak deterrence mechanism. Denial of service is another problem in database security. Weak database audit policy represents a serious organizational risk on many levels. Another threat to the problem of database insecurity is weak system. Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. Strong authentication is therefore required to address these challenges [4].

Database Security Requirements

The basic security requirements of database systems are not unlike those of other computing systems. The basic problems access control, exclusion of spurious data, authentication of users and reliability.

a) **Physical database integrity:** The data of a database are immune to physical problems such as power failures and someone can reconstruct the database reconstruct if it is destroyed through a catastrophe.

b) **Logical database integrity:** The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields.

c) **Audit ability:** It is possible to track who or what has accessed the elements in the database.

d) **Access control:** A user is allowed to access only authorized data and different users can be restricted to different modes of access.

e) **User authentication:** Every user is positively identified, both for the audit trail and for permission to access certain data.

f) **Availability:** Users can access the database in general and all the data for which they are authorized.

Database Security Guidelines

If a database is to serve as a central repository of data, users must be able to trust the accuracy of the data values. This condition implies that the database administrator must be assured that updates are performed only by authorized individuals. The DBMS can require exact user authentication. For example, a DBMS might insist that a user pass both specific password and time-of-day checks. This authentication supplements the authentication performed by the operating system. [1]

Databases are often separated logically by user access privileges. For example, all users can be granted access to general data, but only the personnel department can obtain salary data and only the marketing department can obtain sales data. Databases are very useful because they centralize the storage and maintenance of data. Database integrity concern that the database as a whole is protected against damage, as from the failure of a disk drive or the corruption of the master database index. These concerns are addressed operating system integrity controls and recovery procedures [2].If sensitive data are encrypted, a user who accidentally receives them cannot interpret the data.

Database Security levels

To protect the database, we must take security measures at several levels:

a) People: Users must be authorized carefully to reduce the chance of any such user giving access to an intruder in exchange for a bribe or other favours.

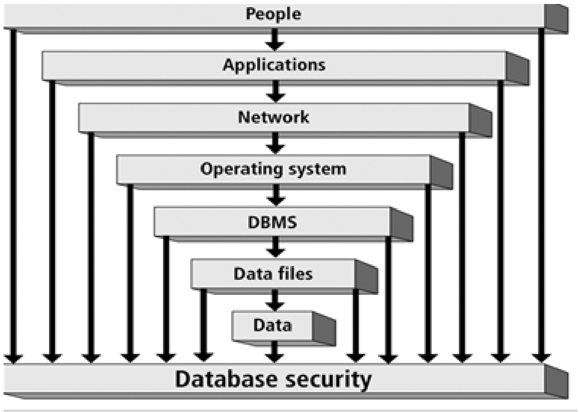

Figure 2: Database Security Levels [2]

b) Operating system: No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.

c) Network: All database systems allow remote access through terminals or networks, software-level security within the network software is as important as physical security, both on the Internet and in networks private to an enterprise.

d) Database System: Some database system users may be authorized to access only a limited portion of the database. Other users may be allowed to issue queries, but may be forbidden to modify the data [2].

Techniques for Database Security

One of the most basic concepts in database security is authentication, which is quite simply the process by which it system verifies a user's identity. A user can respond to a request to authenticate by providing a proof of identity, or an authenticate token. An authenticated user goes through the second layer of security, authorization. Authorization is the process through which system obtains information about the authenticated user, including which database operations that user may perform and which data objects that user may access. A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data they are supposed to see.

Confidentiality has several features like privacy of communications, secure storage of sensitive data, authenticated users and authorization of users. Another technique that can be used to secure database is the use of access control [1]. This is the access to the system is only given after verifying the credentials of the user and only after such verification is done, the access is given. Audit trial is another method that can help in the database security. Audit trial need to be carried to found the history of operations on the database [4]. One of the techniques for achieving security is by using a DBMS for multiple users of different interests is the ability to create a different view for each user.

A. Access Control Mechanisms

Access Control Mechanism is a technique to maintain data confidentiality. When someone tries to access data object, Access Control Mechanism checks the rights of the user against set of authorizations. They are generally specified by security administrator or security officer. Authorizations are given as per the security policy of the organization. Along with Access Control Mechanism, A strong Authentication mechanism is also required to authenticate the valid user of a database system. After that access control will help defining different access permissions on different data objects of a database [6].

B. Techniques to fight with SQLIA

SQLIA is the most dangerous attack on databases. This section discusses some of the techniques to detect and prevent SQLIA. The detection approaches for SQLIA can be categorized broadly into pre-generated and post-generated approaches. Post-generated approaches are generally useful while analyzing dynamic SQL which is generated by web application. Pre-generated approaches are generally used during the testing phase of the web application.

C. Data Encryption

This is the basic technique used for securing any kind of information or data. So this technique can even be applied to databases. Encryption is a process of translating plain text to encoded form called cipher text. This is usually carried out using secret encryption key and cryptographic cipher.

D. Data Scrambling

Data Scrambling is a process of making sensitive information in non-production databases safe for wider visibility [8][9]. Data scrambling is also known as data sanitization, data masking and data obfuscation.

Data scrambling is generally used when users have proper access to data in the database but still it is required to secure sensitive information from them. Examples of such users can be third party developers or testers working on data in database. So the values of the data which are sensitive are changed but still the values are realistic in nature.

Advantages of Database Management System

The user interacts with the database through a program called a database manager or a database management system (DBMS), informally known as a front end. A database administrator is a person who defines the rules that organize the data and also controls who should have access to what parts of the data [1]. A database offers many advantages over a simple file system. It improves data sharing in a way that enables the end users have better access to data that is correctly managed. There is improved data security in that the security is guaranteed and the data privacy is maintained [4].

DBMS has an effect of ensuring that there is promotion of data integration in a whole organization and one can see a bigger picture of all activities [2]. It is also probable that data access is facilitated and could be used to provide quick answers to queries giving out. There is better decision making is achieved due to accuracy, timelessness and validity of the information generated.

Roles of integrity and reliability in Database security

Databases combine data from many sources, and users expect a DBMS to provide access to the data in a reliable way. When software engineers say that software has reliability, they mean that the software runs for very long periods of time without failing. Users certainly expect a DBMS to be reliable, since the data usually are the key to business or organizational needs. Moreover, users entrust their data to a DBMS and rightly expect it to protect the data from loss or damage.

Data integrity refers to reliability and accuracy of the data that is stored and used in business. Data should assist a firm to make the right decision and avoid inconsistencies. Element integrity concern that the value of a specific data element is written or changed only by authorized users. Proper access controls protect a database from corruption by unauthorized users [5]. Users trust the DBMS to maintain their data correctly, so integrity issues are very important to database security.

III. CONCLUSION

Security is an important issue in database management because information stored in a database is very valuable and many time, very sensitive commodity. So the data in a database management system need to be protected from buses and should be protected from unauthorized access and updates. Database Security paper has attempted to explore the issue of threats that may be poised to database system. These include loss of confidentiality plus loss of integrity. The paper has also discussed areas concerning techniques to encounter any issue of threat using views and authentication. Another method is through back-up methods which ensure that the information is stored elsewhere and recovered in case of failure and attacks. This paper has also discussed the various requirements necessary for the database security and the various levels of security.

IV. FUTURE SCOPE

This review paper will be helpful to the research beginners that develop their own security solutions and basic security control for their database systems. The attacks on databases are also increasing as they are very dangerous form of attack. They reveal key or important data to the attacker. Various attacks on databases are discussed in this paper. Review of some important database security techniques like access control, techniques against SQLIA, encryption and data scrambling. Even some future research areas in the field of database security are also discussed in this paper. This research will lead to more concrete solution for database security issue. In future using this review paper various applications of database security will use the advanced technologies that support the design, implementation, and operation of data management system include security and privacy function and give the assurance that implemented data management systems meet their security and privacy requirement.

REFRENCES

[1] “Security in Computing” 4th edition Mr. Charles P.Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pfleeger.

[2] Bertino et al Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.

[3] http://www.imperva.com/downloads/Top Ten Database Security Threats.pdf

[4] S. Singh, Database System: Concepts, Design and applications New Delhi: Pearson Education India, 2009.

[5] S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.

[6] http://www.appsecinc.com/downloads/Risksto Database Security in 2012.pdf.

[7] Emil Burtescu, “DATABASE SECURITY ATTACKS AND CONTROL METHODS”, Quantitative Methods, Vol. 4, no. 4, Winter 2009.

[8] A NET 2000 Ltd., **“**Data Sanitization techniques‖, A White Paper(2010), Website, September,http://www.datamasker.com/datasanitization_whitepaper.pdf

[9] A NET 2000 Ltd., **“**Data Scrambling Issues‖, A White Paper(2010), Website, http://www.datamasker.com/datascramblingissues.pdf

[10] Huw Price, **“**A Short Guide to Scrambling, Masking and Obfuscating Production Data, Grid Tools‖ White Paper, Website, October 15 2012, http://www.grid-tools.com/download/Data_Masking.pdf