Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 2, February 2013, pg.102 – 105

RESEARCH ARTICLE

Database Security

Sukhdev Singh Ghuman

SBDSM Khalsa College Domeli (Kapurthala)

Abstract-- Data security is an emerging concern which is attracting a lot of attention. Its need can be judged by the increase in the number of reported cases of loss of or exposure to sensitive data by some unauthorized sources. Security is a composed part in which it protects and secures the sensitive data or database management software from some unauthorized user or from malicious attacks. In this paper I will be presenting some of the common security techniques for the data that can be implemented for securing and strengthening the databases.

I. INTRODUCTION

All organizations depend on computerized information systems for carrying out their daily activities. All this is done with the help of a database. A database can be defined as a collection of related data, where data are facts that have an implicit meaning. For example, student roll number, name and other details can be recorded in the database. It is built to store logically interrelated data representing some aspects of the real world, which must be collected, processed, and made accessible to a given user population. The collection of software programs that provide the functionalities for defining, maintaining, and accessing data stored in a database is called a database management system (DBMS).There are three level of DBMS abstraction external level, conceptual level and internal level. DBMS should also provide the security besides access and manipulation of data.[1]

II. DIFFERENT TYPES OF ATTACKS

Different types of attacks that can be carried out by an attacker after breaching through all layer of security are [5]:

© 2013, IJCSMC All Rights Reserved

Direct attacks:

Directly hitting the target data is known as direct attack. These attacks are accessible and successful only if the database does not accommodate any protection system.

Indirect attacks:

As its name implies indirect attacks are not directly executed on the target but data from or about the target can be collected through other transitional objects. For purpose to cheat the security system, some of the combinations of different queries are used. These kinds of attacks are difficult to track.

Passive Attack [6]:

In this attack, attacker only inspects data present in the database and do not perform any alteration. Passive attack can be carried out in following ways:

1) Static leakage: In this attack, information about database plaintext values can be attained by examining the snapshot of database at a particular time.

2) Linkage leakage: in this information about plain text values can be achieve by linking the database values to position of those values in index.

3) Dynamic leakage: changes performed in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

Active Attacks:

In active attack, actual database values are modified. [7]These are more problematic than passive attacks because they can misguide a user. For example a user capturing wrong information by the result of a query. [6] There are various ways of performing such kind of attack which are mentioned below:

1) Spoofing – In this attack, cipher text value is replaced by a generated value.

2) Splicing – in this, a cipher text value is replaced by different cipher text value.

3) Replay – It is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

III. DATABASE SECURITY

Database security is a vast concept, some of the important security concepts are discussed in this paper. The important database constructs include access control, application access, vulnerability, interference and auditing mechanism. [2]

Access Control

Access control policies helps in making the rules according to which access to the database objects is regulated. Discretionary Access Control is the most commonly used method of access control.

© 2013, IJCSMC All Rights Reserved

Discretionary access control policies are based on authorization rules. An authorization rule states that a subject has the privilege to exercise a given action on a given object. [1]

Inference Policy

This is essential to protect the data at some specific level. It comes when the analysis of particular data in the form of facts are required to be prevented at a certain higher security level. Inference policy also helps to determines how to protect the information from being released.

User Identification /Authentication

This is the very basic obligation to ensure security since the identification process defines a set of people that are allowed to access data. To ensure security, the identity is authenticated and it keeps the sensitive data secure and from being modified by unauthorized user.

Accountability and auditing

Accountability and audit checks are needed to ensure physical integrity of the data which requires defined access to the databases and that is handled through auditing and for keeping the records. The data puts on servers for authentication, accounting and access of a user can be analysed with the help of auditing and accountability.

Encryption

Encryption is the process of converting information into a cipher or a code so that it cannot be readable to all other people except those who hold a key for the cipher text. The cipher text or encoded text is called as encrypted data.

IV. CONCLUSIONS

Database security presents features that must be seriously taken into account. The first option, for a secure database is represented by its optimal protection. Ensuring database security must be done from outside to inside, this involving ensuring security starting from the physical level and ending with the data level (physical, network, host, applications and data). Databases are a favourite target for attackers because of the data these are containing and also because of their volume. Data warehouse is the ultimate goal. Efforts to ensure database security are considerably higher than for the other types of data. It is easier to implement an access list for a great number of files than an access list for the elements of a database. Database security mechanisms should not irritate their users. Data to any organization is a most important property. Protection of crucial data is always a tough task for an organization at any stage. Database can be accommodated in several ways. Different types of attacks and threats are there today from which a database should be protected.

© 2013, IJCSMC All Rights Reserved

References

[1] Sabrina De Capitani di Vimercati, Pierangela Samarati, Sushil Jajodia, “Database Security”

[2] Meg Coffin Murray Kennesaw, “Database Security: What Students Need to Know”, Journal of Information Technology Education: Volume 9, 2010

[3] Paul Lesov, “Database Security: Historical Perspective ”

[5] Emil Burtescu, “DATABASE SECURITY - ATTACKS AND CONTROL METHODS”, Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009

[6] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, “Review of Attacks on Databases and Database Security Techniques”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[7] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer, “Database Encryption – An Overview of Contemporary Challenges and Design Considerations”, SIGMOD Record, September 2009 (Vol. 38, No. 3).

© 2013, IJCSMC All Rights Reserved