Security Of An Enterprise Level Rdbms - Threats And Challenges

Ch Sajjad Ahmed, Saeed ur Rehman Malik

Abstract: All enterprises are managing their day to day affairs using IT based applications. In these applications, the most valuable asset is Data. A Relational Database Management System is utilized to retrieve and maintain the data in an efficient manner. (RDBMS)[1] was coined in Late-Seventies by E.F. Codd and since then all commercial and enterprise database are following RDBMS Model. Importance of data and its volume make RDBMS favorite targets for attackers. These attacks can result in compromise of a Database in many ways. In this paper the challenges and threats being faced by RDBMS are identified.

Key Words : RDBMS, Database security, challenges, threats, attacks

1 INTRODUCTION

Information or data is the most valuable asset of any business. In today's world every organization, irrespective of their role or business, has automated information systems. All such information systems have underlying RDMBS for storing and retrieval of information or data. Security of data stored in these RDBMS is very crucial for business of such organizations. Aspect of security gets more important if data stored is defence or military related. Thus understanding database security and challenges being faced by RDBMS is of prime importance to take necessary safeguards.

2 ORGANIZATION OF PAPER

The paper is organized in three sections. In section 1 concept of Database Security is briefly covered. In section 2, Threats and Challenges to RDBMS are discussed. Conclusion and future work is given in section 3.

3 DATABASE SECURITY

Database security can be defined as a system of ensuring three basic concepts of Information Security i.e., Confidentiality, Integrity, and Availability, or CIA of the database can be protected. (Fig 1). Unauthorized entry or access to a database server/ information stored in the database signifies a loss of confidentiality; alteration of data by unauthorized individuals/ process leads signifies loss of integrity; and unavailability of database services to authorized users, when needed signifies loss of availability. Loss of any one or more of these basic facets of database security will have a significant impact on its security [2].

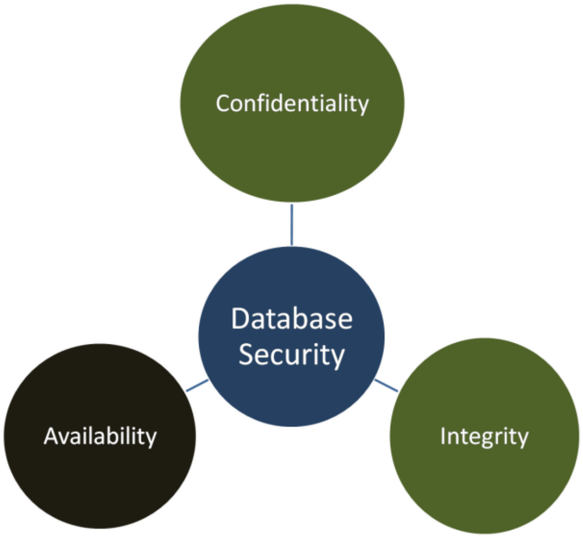

Fig 1: *Components of Database Security*

Security of the Database cannot be ignored in the competitive world of today, which demands controlling user actions on the database on the database and the objects inside it, within the confided boundaries of authorization. Implementation of desired level of security is basic requirement of organizations running successfully. No organization can afford unauthorized access or changes in their database. Resultantly, direct access of database is restricted to minimum users only. Accidental or malicious modification of data is another major concern. The organizations demand protections against any such change. Protection of data and its confidentiality are the prime security concerns. Application of security on database is implemented in layers which are: Database Administrator, System Administrator, Security Officer, Developers and Employee [2]. Any of these layers can be exploited by an attacker to breach the security of RDBMS. Based on these layers, an attacker can be classified into following three categories [3]:-

a. **<u>Intruder</u>**. An unauthorized user who uses illegal means for accessing a computer system or a database, with an aim to obtain valuable information.
b. **<u>Insider</u>**. A member of trusted users who abuses his/ her privileges in an effort to get information which is beyond his/ her own access rights.
c. **<u>Administrator</u>**. A person with privileges to carry out administrative tasks on a computer or database system but exploits these privileges to access information/ data

- *Ch Sajjad Ahmed is a Professional Engineer possessing BE (Computer System Engineering) from NUST Pakistan and MS in Computer Engineering from UET, Taxilla Pakistan. PH +923214688829. E-mail: csajjadahmed@gmail.com*
- *Saeed ur Rehman is a Professional Engineer possessing BE (Electric Engineering) from NUST Pakistan and MS in Electric Engineering from UET Taxilla Pakistan. PH +923331403108. E-mail: saeedurrehmanmalik@gmail.com*

which is illegal in accordance with the rules of organization.

An attacker, after having intruded through all levels of protection and reached the database, will try a series of attacks progressively which can be **direct** or **indirect** or it can be carried out **by tracking** [4].

a. Direct attacks are obvious attacks which succeed only if there is no protection mechanism implemented on database. If the attacker achieves desired results he utilized the data obtained, however, if direct attack fails, then the attacker moves to next approach i.e., indirect attack.
b. Indirect attacks are not executed on the target directly. The attack is based on the information from or about the target through intermediate objects. Combination of queries is used, some of which is focused on cheating the security mechanism in place.
c. Incase direct and indirect attacks fail to achieve desired result, tracking attack is applied to the databases. These are tried on databases having suppression mechanism in place. These type of attacks are successful against databases having short answers to queries. These attacks are based on a simple principle i.e. if a direct query has as result a small number of answers, the denial of the main claim will result in zero. In literature, this type of attack is called Linear System Vulnerability.

Attacks on database can also be classified into passive and active attacks [5]:-

a. **Passive Attack**. In passive attack, attacker does not perform any direct action on the database. He only observes data present in the database. Such attack can be carried out in following three ways:-
   (1) **Static Leakage**. In this type of attack, snapshot of database at a particular time is observed to gain information about values stored as plain text.
   (2) **Linkage Leakage**. In linkage leakage, database values to the position of values in index are linked to obtain information about values stored as plain text.
   (3) **Dynamic Leakage**. In Dynamic Leakage, information about plain text values is obtained by observing and analyzing the changes that take place in database over a period of time.
b. **Active Attack**. In active attack, direct activity is performed on database changing/ modifying the database values [3]. Active attacks are more severe than passive attacks as they mislead users by presenting incorrect data or results of query [5]. These attacks can be performed by replacing cipher text with:-
   (1) **Spoofing**. Generated values replace cipher text.
   (2) **Splicing**. Replacing cipher text with different cipher text value.
   (3) **Replay**. Cipher text is replaced with older version if cipher text which was deleted or replaced.

4 THREATS AND CHALLENGES BEING FACED BY RDBMS

The enterprise level database management system and its infrastructure are subject to a wide range of threats. In this section, serious threats, envisages in an enterprise database will be highlighted.

a. **Excessive Privilege Abuse**. Excessive Privilege Abuse occurs when the users or applications are granted access levels, which are beyond required to perform their assigned functions. The intentions of exploiting excessive privileges can be malicious. For example, a user in an organization, responsible to update contact information of employees can use the excessive privileges to change salary information [6].
b. **Legitimate Privilege Abuse**. Legitimate Privilege Abuse occurs if a user utilizes his legitimate database privileges to perform unauthorized activities, forbidden or restricted according to the organization's rules [6].
c. **Privilege Escalation**. Privilege Escalation occurs when a user exploits vulnerabilities of software to escalate his privileges from limited user to administrator privileges [6]. The escalated user account can be utilized for creation of additional/ bogus accounts, transfer of funds and misinterpret certain sensitive information. Rootkit is a procedure hidden in the database that provide administrative or administrative level privileges in accessing the database, which can even suppress the alerts generated by Intrusion Prevention System (IPS). The rootkits can be installed only when the security offered by underlying operating system is compromised [7].
d. **Platform Vulnerabilities**. As the database is installed on an underlying operating system, the security vulnerabilities of security system also contribute to threat/ compromise of database. These vulnerabilities, along with the vulnerabilities of softwares/ services installed on the system, if successfully exploited by the attacker can achieve desired results for the attacker, which include unauthorized access, data corruption, or denial of service. For example, the Blaster Worm took advantage of a Windows 2000 vulnerability to create denial of service conditions [6].
e. **Inference**. Even a secure database manager possibly provides information to the users to draw inferences. By drawing inference it is meant that the user guesses or concludes the information which is more sensitive on the basis of information obtained from database. Some prior knowledge of the user can also be beneficial in this regard. If the drawn inference or guessed information pertains high security classification then a information security breach is said to have occurred. Major problems that arise when the user is able to draw inferences, on the basis of information collected from Database, are as under [8].
   (1) **Aggregation Problem**. Aggregation problem occurs when the bits and pieces of information collected by the user does not have a major impact but once these pieces are put together, the obtained result is of much high value e.g., if a person is able to know the profit earned by some branches of an organization, it may have minor impact but if the user can calculate the profit of entire organization, the information is having much amplified impact.
   (2) **Data Association Problem**. Data association problem occurs when different attributes, if seen together, present a higher level of classification than viewing each attribute separately. For example, the salaries of all the employees of an organization is having less security value. Same is the case with the list of employees of an organization. However, when both the attributes are combines, i.e., list of employees and their salaries, the

information has much bigger impact and thus high security value.

f. **SQL Injection**. In SQL injection, SQL statements are altered by the users by injection of SQL commands through web page input. The injected SQL commands alter the SQL statements resulting in compromising the security of RDBMS utilized to serve the web application. [9].

g. **Unpatched RDBMS**. Security of software is never absolute. Weaknesses are continuously indentified and security patches are released to address the security vulnerabilities. Therefore, if the database or its underlying operating system is not patched to latest security patches, it provides an easy opportunity to the attackers. Leaving the DBMS un-patched, after release of security patches renders the system further exploitable owing to available literature regarding information security weaknesses fixed by the patch. The attackers use this information to exploit unpatched databases [7].

h. **Unnecessary RDBMS Features Enabled**. All the RDBMS come with a standard set of features and functionalities required to fulfill the requirement of varied customers and applications. A particular system or application may not be requiring all these services to be enabled. All such services which are not required for operations of specific system/ database shall be disabled to avoid their exploitation by the attackers [6].

i. **Mis-configurations**. All the configurations including the database parameters shall be finalized and implemented with utmost care. Any unnecessary features left on contributes to weakening the security level of database [6]. Attackers have identified these incorrect configurations supporting certain types of attacks. Thus the mis-configurations are exploited to gain desired results which may include gaining access to encrypted files or resetting default configurations. Therefore unpatched system and services may result in disclosure of information to unauthorized users [8].

j. **Weak Audit Trails**. A database audit policy ensures automated, timely and proper recording of database transactions [6]. This policy provides the details of actions performed on database, by whom and when. Such a trial shall always be an important consideration while finalizing database security consideration as all the actions performed on database shall be traceable and the users performing them be accountable. Weak policy of maintaining audit trails will pose a serious risk to organization's database along with posing stability issues in its operations [2].

k. **Denial of Service**. In this type of attack all users (including legitimate users) are denied access to data in the database. Denial of service (DOS) conditions may be created via many techniques - many of which are related to the other mentioned vulnerabilities. For example, DOS may be achieved by taking advantage of a database platform vulnerability to crash a database server. Other common DOS techniques include data corruption, network flooding, and server resource overload (memory, CPU, etc.) [6].

l. **Database Communication Protocol Vulnerabilities**. Large number of security weaknesses are being identified in the database communication protocols of all database retailers. Fraudulent activities directing these vulnerabilities can vary from illegal data access to data exploitation and denial of service and many more [2].

m. **Insider Mistakes**. Some attacks are not intentional, they just happen unknowingly, by mistake. This type of attack can be called as “unintentional authorized user attack” or insider mistake. It can occur in two situations.

(1) The first one is when an authorized user inadvertently accesses sensitive data and mistakenly modifies or deletes the information.

(2) The latter can occur accidentally when a user makes an unauthorized copy of sensitive information for the purpose of backup or “taking work home.” Although it is not a malicious act, but the organizational security policies are being violated and results in data residing on a storage device which, if compromised, could lead to an unintentional security breach. For example a laptop containing sensitive information can be stolen.

n. **Weak Authentication**. Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.

(1) **Brute Force**. In this strategy, attacker repeatedly enters username/password combinations until he finds the correct one. The brute force process may involve simple guesswork systematic enumeration of all possible username/password combinations. The attacker can often use automated programs to accelerate the brute force process.

(2) **Direct Credential Theft**. An attacker may steal login credentials from the authorized user.

o. **Backup Data Exposure**. Backup database storage media is often completely unprotected from an attack as well as a natural calamity like flood, earthquake etc. As a result, several high profile security breaches have involved theft of database backup tapes and hard disks [6].

5 Conclusion and Future Work

In enterprise level application architecture; database is the most vulnerable component. In this study, an effort is made to briefly explain major challenges and threats being faced in RDBMS. As a future task, a comparative analysis will be carried out between different measures and techniques for enhancing security of RDBMS.

REFERENCES

[1] C.F Codd, “ A RELATIONAL MODEL OF DATA FOR LARGE SHARED DATA BANK”, Communication of ACM, Vol 13, No 6, 1970, Pages 377-87

[2] http://www.brighthub.com/computing/smb-security/articles/61400.aspx (20 Nov 2014)

[3] ErezShmueli, Ronen Vaisenberg, Yuval Elovici, ChananGlezer, “Database Encryption – AN OVERVIEW OF CONTEMPORARY CHALLENGES AND DESIGN CONSIDERATIONS”, SIGMOD Record, September 2009 (Vol. 38, No. 3).

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

[5] Mr. SaurabhKulkarni, Dr. SiddhalingUrolagin, “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

[6] Amichai Shulman, White Paper “TOP TEN DATABASE SECURITY THREATS”, ImpervaInc

[7] http://www.channelinsider.com/c/a/Security/Database-Vulnerabilities-Top-10-Rules-IT-Shops-Break-772412 (18 Nov 2014)

[8] Ravi S. Sandhu, SushilJajodia, “DATA AND DATABASE SECURITY AND CONTROLS”, Handbook of Information Security Management, Auerbach Publishers, 1993, pages 481-499.

[9] http://www.w3schools.com/sql/sql_injection.asp (18 Nov 2014)