Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 05, May -2019

A STUDY ON DATABASE SECURITY THREATS AND MECHANISMS

Rishabh Sinha[1]

[1]*Research Scholar (MBA Tech), IT & Marketing Department, SVKM"s NMIMS MPSTME, Mumbai, India*

Abstract: *The heart of secure systems lies in protecting data and most of the users usually rely on database management systems or DBMS for managing this protection. The security of databases is more of a recent development as compared to the programming and operating systems. Databases play an important role in many business, government and private organizations. They are used for making the retrieval and maintenance of data quite easy and become efficient when the data is stored in databases. The basic requirements for any database systems aren't like other computing systems. The major systems faced for databases include access control, authentication process of users and their benefits. Several security mechanisms are being used for storing and securing the large volumes of data. The reason why databases are attacked so often is due to the fact that the databases contain large volume of data stored in them. This paper discusses the various security mechanisms used. Further this paper also discusses about some of the major threats and challenges in database security.*

Keywords: *Database Security, Attacks, Encryption, Integrity, Threats*

1. Introduction

In today' time, data is considered to be the most valuable asset, be it an individual or an organization. Data has played a major role in determining the success of any organization. The goal for any organization relies heavily on the quality and quantity of the data that it holds. In order to make the retrieval and maintenance process easier, data is now being stored in the form of databases.

Databases play an essential role for any government and business organizations and tend to hold data that is reengineered for making it more effective with a new set of revised goals. The task of security for today' time has become a major concern for any data engineer and people from all over the world are concerned for implementing strong data security mechanisms to protect their confidential data.
For any database, there are various levels and these levels include-

i. ***Database Administrator***
ii. ***System Administrator***
iii. ***Security Officer***
iv. ***Developers***
v. ***Employees of the organization.***

The data-security can be breached any of the above stated levels by an attacker.

Types of Database Attackers: A database attacker can be broadly classified into the following three categories-

i. **Intruder:**
An intruder refers to an unauthorized user that illegally accesses the computer system and then tries to extract the valuable information from the host system

ii. **Insider:**
An insider is the person who belongs to the group of users, that are trusted and thus make abuse of the privileges given and tries to gain control over the information using own access rights

iii. **Administrator:**
An administrator is a person, who has privileges of administering a computer system, but instead he users his administrative privileges illegally in terms of security policy of an organization to spy on the database systems behavior and getting valuable information

2. Types of Attacks

A database attacker post breaching through all the levels of protection can carry out any of the following two types of attacks-

i. **Direct Attacks:**
In case of a direct attack, the target database is attacked directly. These are some of the obvious attacks and can be successful only when the databases don't implement any sort of protection mechanisms

ii. **Indirect Attacks:**
The indirect attacks are the attacks that aren't directly executed on the targeted site, but the information about the target, can be obtained from the intermediate objects. Various combinations of queries are often used and some of these are used for the purpose to cheat the security mechanisms. The indirect attacks are difficult to track

3. Classification of Database Attacks

The attacks on a database can also be further classified into the following categories-

i. **Passive Attacks:**
In case of passive attacks, the attacker has the tendency to observe the data that is present in the database.
The passive attacks can be carried out in the following three ways-

a. **Static Leakages:** In this type of attack, the information about plaintexts of database can be obtained by observing the snapshots of the database at a given particular time

b. **Linkage Leakages:** In this type of such attack, the information regarding the plain text values are obtained by the means of linking the database values to the position of the values present in the index

c. **Dynamic Leakages:** In this type of attack, the changes are performed in the databases for a period of time and these changes can be observed and analyzed as well as information about the plain texts can be obtained

ii. **Active Attacks:**
In case of an active attack, the actual database values are modified. These are proven to be more problematic as compared to the passive attacks because of the fact that they can be misled by nay user.
Following are the methods listed for carrying out an active attack on the database-

a. **Spoofing:** In case of spoofing, the ciphered or encrypted text value is usually replaced by a generated value

b. **Splicing:** Here, the cipher text value is replaced by a different cipher text value

c. **Replay:** Replay refers to such a kind of attack, where in the cipher text value is often replaced by an old version that has been previously deleted or updated

iii. **Inference:**
Inference is a major attack on any database system. It is a way of deriving sensitive data from a non-sensitive data. A direct attack is high on possibility. In this type of attack, the query field is very specific and the query matches with exactly one data item. In case of an indirect attack on the database under the inference, includes use of statistical data for getting the sensitive information. This attack can be carried out in many ways. The attacker can try to infer the sensitive information based on sum of some values that are used in reports. The use of **COUNT** along with **SUM** function could be used for getting sensitive information. The **SUM** and **COUNT** functions are commonly used functions as they are by default provided under the aggregate functions by the Database Management Systems. The attackers can use the **MEDIANS** as a statistical measure in order to determine the actual sensitive value. This process happens to be slightly difficult and so, the attacker finds selections that have only one point of intersection, which lies exactly in the middle.

There is another type of possible attack under the Inference attacks, known as the **Tracker Attacks**. In case of the tracker attacks, a desired data can be recorded by using the additional queries that can lead to producing small results. The attacker adds two additional records that are to be retrieved for two different set of queries, so that these two additional data sets cancel out each other and thus only the desired data is left.

The third type of data that falls under the inference is called the **Linear System Vulnerability**. This attack requires little bit of algebraic logic for finding the data distribution in a database and thereby using it to find the desired elements. Instead of using two opposite query sets, a unique set of queries can be used which would be cancelling the effect of each other and thus the final desired information is found.

iv. SQLIA:

SQLIA stands for **SQL Injection Attack**. It is also known as SIA. Most of the web applications often use the on-fly SQL queries without applying any proper input validation of the user. This forms the basic reason for SQLIA. The attackers can make the server run malicious SQL queries and can manipulate the databases. The SQLIA is considered to be the most dangerous type of attack on the databases.
The SQL Injection Attacks can be classified into the following categories-

a. **Bypassing Web Authentication:** In this case, the attacker uses the input field which is used in the **WHERE** condition of the query
b. **Database Fingerprinting:** In this type of attack, the attacker generates logically incorrect or illegal queries. This forces the DBMS to throw the error messages. These error messages include tables, stored procedures, views etc. Based on the error, the message attacker can guess the database that is being used by the applications as different databases have different style of error reporting
c. **Injection using UNION Query:** In this type of attack, the user obtains data from a table that is different from the one intended by the developer
d. **Damaging Using Additional Injected Query:** In this type of attack, the attacker enters the input in such a way that the additional query along with the original query is generated
e. **Remote Execution of Stored Procedures:** In this type of attack, the attacker often executes some stored procedures that can cause harmful effects post-execution

Apart from the above stated attacks, any legitimate user can take the advantage of the access rights that are given to him/her and thus can expose the sensitive information to the attacker or the illegal users of the system, that are either within or outside the organization. Such attacks are dangerous in case of the defense organizations, as their data is extremely sensitive and can trigger to large amount of destruction. Commercial organizations such as the manufacturing firms, financial firms and banks have large amount of sensitive information that can be used by the attacker for the purpose of illegal means. It may cause harm to organization in terms of profit as well as it may be harmful to the customers as well for such organizations.

4. Most Common Database Security Issues

Following are the most common security issues faced in databases-

i. Excessive Permissions:

A significant number of databases have large number of accounts with role of DBA assigned, it is found that a majority of user accounts contain the default privileges or were granted roles that had access to the unnecessary functionality

ii. Weak Passwords:

A number of databases have users that have either weak or default passwords. Weak credentials for any database are becoming a problem for every organization. Systems that don’t enforce a strong password policy can be easily compromised. A weak password policy also indicates that the other systems inside the network might have weak credentials, expanding the attack surface for the attacker. These passwords can be easily guessed or a brute force may allow an attacker the privileged access to the database

iii. Missing Patches:

Some databases had missing security updates or were running older versions of the software. This gives rise to an alarming question: “is it the fault of owners and administrators that they are finding it too difficult to apply the relevant patches, or the organizations support a patch-management policy?” These missing patches could prove to be extremely worrying for database administrators

iv. Poor Auditing:

A large number of databases have been found with incorrect configuration for logging or auditing activities. This is a features that all the databases house in order to track and audit the events such as data modifications and accesses. The absence of tracking events to sensitive data on a production system could lead to difficulty in discovering what activity has taken place on the database at the time of any data breach. This is considered to be a low-risk, however auditing needs to be included whenever a database is build

v. Default Account Names:

Some of the databases have been found that contain default accounts. As a part of the defense in depth strategy, it is always recommended the default accounts should be renamed and locked wherever possible, as there are chances that they could be used as a target of brute-force or even password guessing attack

vi. Excessive Number of Stored Procedures:

Few databases have been found to have large number potentially dangerous stored procedures, including those that can run a system command or access file on the underlying OS (operating systems). This issue is considered to offer a risk on the security posture for any database, as the stored procedures effectively increase the functionality available, which could be leveraged for launching attacks against an underlying operating system of the host and even against other hosts that are present on the network

vii. SSL Not Enabled:

A certain number of databases have accepted connection over clear text channels, and if the attacker has an access to the network and is able to sniff through the network traffic, then this results in confidentiality and integrity of transmission

viii. Blank Passwords:

Some databases have been found that they are configured to allow the blank passwords. It is however similar to the case of weak password issue, but none of the databases under weak password had actually configured with the a blank password

ix. Duplicate Passwords:

Some databases even have users configured with a duplicate password. This indicates that a single default password is used at the time of account creation. There is also a high possibility that users aren’t educated about how to create a strong password or even in worse case change their password

x. Primary Account Number in Clear Text:

Lastly, a small portion of databases were found to be containing the Primary Account Number or PAN’s written in clear text. It should be made sure that all the sensitive information such as PAN is stored only in an encrypted format in the database

5. Database Security Considerations

In order to eliminate the security threats every organization needs to define a security policy and also that should be strictly enforced. A strong policy should also be strictly enforced.

i. Access Control:

Access control ensures that all the communication taking place within the database and other system objects are according to the policies and controls defined. This makes sure that no interference occurs by any attacker neither internally nor externally and thus, protects the databases from potential errors that can make an impact as huge as stopping the operations of firms. Access controls also helps in minimizing the risks that may directly have an impact on the database present on the main servers

ii. Inference Policy:

It is required to protect the data at a given certain level. It can occur with interpretations from certain data in the form of analysis or facts that are required to be protected at higher security levels. It further determines how to protect the information from being disclosed

iii. User Identification Authentication:

User identification and authentication forms the basic necessity for ensuring the security, as the identification method is used for defining a set of people that have been allowed to access data and provide a complete accessibility mechanism. In order to ensure security, the identity is authenticated and the sensitive data is kept safe from being modified by any ordinary user

iv. Accountability and Auditing:

Accountability and audit checks are required for ensuring the physical integrity of data that requires a defined access to the databases and this is managed through auditing and record keeping. It also helps in analyzing the information held on the servers for the purpose of authentication, accounting and access of users

v. Encryption:

Encryption is the basic technique used for securing any kind of information or data and can be applied on the databases as well.

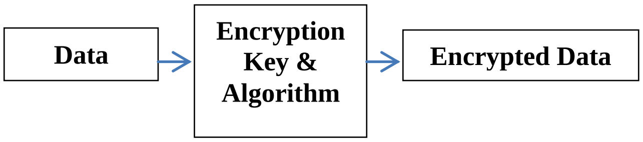

Fig 1: Encryption Process

Encryption is a process of translating a plain text to an encoded form known as the cipher text or a code in order to make it unreadable to all other people except for those having the key to the information. The resulting encoded information is known as the encrypted information and is carried out using a secret encryption key and a cryptographic cipher. Data is encrypted using encryption keys and algorithms. The encrypted data is then stored in database and then decrypted when needed for processing purpose.

There are two commonly used methods for data encryption, namely- Symmetric Encryption and Asymmetric Encryption.

Symmetric Encryption: In case of symmetric encryption, a single key is used for both encryption and decryption.
Asymmetric Encryption: In this type of encryption technique, a pair of secret keys is used. One of the key is used for encryption and the other one is used for decryption.

While performing the database encryption, a decision has to be made regarding where to perform the encryption- inside or outside the database. Some key issues are also involved in this technique such as- ***How to secure the keys from an attacker of the system? How to give the administrative rights of manipulating the data by the use of keys?*** And lastly, ***How to provide the limited access for these keys?***

It is also important to provide a proper authentication mechanism, as in their absence, it becomes easy to get the access to the keys by the use of social engineering techniques. The implementation of encryption decisions is very important in line with the improved protection. By developing the encryption strategies, some important questions also arise such as *how, when and where* would the encryption will be performed?

vi. Data Scrambling:

Data scrambling refers to the process of making sensitive information in non-productive databases safer for a wider visibility. This method is also known as data sanitization, data masking or data obfuscation. This is generally used when users have a proper access to the data present in the database, but still is required for securing the sensitive information from. Some examples of such type of users include the third party developers or testers that are working on the database data. So, the values of this data that is sensitive, is changed and still the values present are realistic in nature. The main secure methods of scrambling include extracting the data through the use of scrambling functions on either the live copy or a reporting copy of the production data by building a set of views, which can be used for masking the data and creating a secure environment, then taking copy of the production data, updating the data and then a complete copy to develop.

One of the core benefits of scrambling is **traceability,** which becomes important in case of a data loss. Scrambling is more through and more useful to the testing teams. Scrambling for new releases of software is automatically upgraded as part of the normal life cycle.

Some issues are also involved in this method. One of the key concerns of scrambling is that the scrambled data should resemble the original data. Contents present in one column in row are related to the contents present in the other columns of the same row. Scrambled values should also maintain certain type of relationships. Rows in the table are de-normalized and contain information that is usually identical among the many rows. Sometimes data is masked which can be used as the join key for columns in many other tables.

6. Conclusion

Databases are the backbone for a number of applications in today's time. They are the primary form of storage for many organizations. As the data is constantly increasing, the number of attacks on database is also increasing. Also, databases act as a soft target for their attackers because of the large volume of data. The databases need to implement strong security mechanisms for protecting the data. The various attacks on the database and their counterattacks have also covered in this paper.

References:

[1]Akanji (et. Al): "A Comparative Study of Attacks on Databases and Database Security Techniques", African Journal of Computing and ICT (2014)

[2]Gaikwad (et. Al): "A Review of Database Security", International Journal of Science and Research (Volume 3 Issue 4, April 2014)

[3]Singh S. (et. Al): "A Review Report on Social Threats on Database", International Journal of Computer Science and Information Technologies (Volume 5 (3), 2014) Pages 3215-3219

[4]Monika Jain: "Attacks on database and security", International Journal of Academic Research and Development (Volume 1 Issue 5, May 2016)

[5]Malik (et. Al): "Database Security-Attacks and Control Methods", International Journal of Information Sciences and Techniques (Volume 6, Number ½, March 2016)

[6]Rohilla (et. Al): "Database Security: Threats and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering (Volume 3 Issue 5, May 2013)

[7] Deepika (et. Al): "Database Security: Threats and Security Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (Volume 5 Issue 5, May 2015)