A Review Report on Database Security – Attacks and control Methods

Dileep Kumar Rawat[1], Ram Singar Verma[2]
[1]Student, [2]Assistent Professor
Dept. Of Computer Science, CET (UIET)
Babasaheb Bhimrao Ambedker University, Luck now, India

ABSTRACT: Database, which is collection of huge sensitive and important data. So, Security of data and database has become an important issue in technical world. Database often hold the backbone of an organization. Its transactions, customers, employee info, financial data for both the company and its customers and much more. So, in this paper we have focus on attacks related to database as well as several control methods and techniques related to database security and now cryptography is used at different levels to provide security.

KEYWORDS: **Attacks, Security, Threats, DBMS, Database, Cryptography.**

I. INTRODUCTION

Information or data is one of the most valuable assets in any organization. Almost all organization like social, governmental, educational etc…have now automated their information system and other operational or non-operational working function. They have maintained database that contains important and sensitive data so database security is very important and serious issues in technical world. Now we shall first discuss what is Database Security?

1.1Database Security

Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment.

1.2 Database security considerations

To eliminate the security threats every organization must define a security rules and conditions. And that security rules should be strictly enforced. A strong security rules must contain well defined security features.

1.2.1 Access Control

Access control is responsible for control of rules determined by security policies for all direct accesses to the system. Traditional control systems work with notions subject, object and operation. For better image look at the figure of secure DBMS.

1.2.2. Inference Policy

An Inference policy is a data mining technique performed by analyzing data in order to illegitimately gain knowledge about a subject or database. An Inference attack occurs when a user is able to infer from trivial information more robust information about a database without directly accessing it.

1.2.3. User Identification/Authentication

User identification (user ID) is a logical entity used to identify a user on a software, system, and website or within any generic IT environment. It is used within any IT enabled system to identify and distinguish between the users who access or use it. Authentication is the process of confirming that a user logs in only in accordance with the rights to perform the activities he is authorized to perform. User authentication can be performed at operating system level or database level itself. By using authentication tools for biometrics such as retina and figure prints are in use to keep the database from hackers or malicious users.

1.2.4. Accountability and Auditing

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

1.2.5. Encryption

Encryption is the process of encoding or transforming information by means of a cipher or a code so that it becomes unreadable to all other people except those who hold a key to the information. The resulting encoded information is called as encrypted information.

1.3. Cryptography

Cryptography is the science of encoding information before sending via unreliable communication paths so that only an authorized receiver can decode and use it. The coded message is called cipher text and the original message is called plain text. The process of converting plain text to cipher text by the sender is called encoding or encryption. The process of converting cipher text to plain text by the receiver is called decoding or decryption.

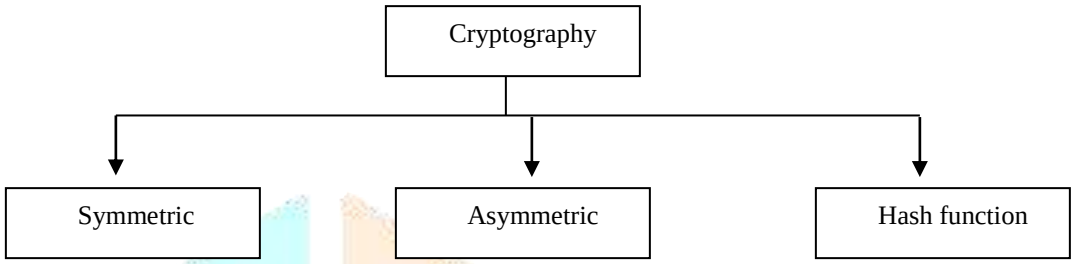

Figure 1 : Cryptography

1.3.1. Semmetric-key cryptography

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text.

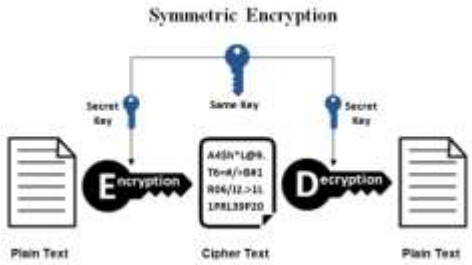

Figure 2 : Symmetric Cryptography

1.3.2 Asymmetric-key cryptography

Public key cryptography, or asymmetrical cryptography, is any cryptographic system that uses pairs of keys *public keys* which may be disseminated widely, and *private keys* which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key

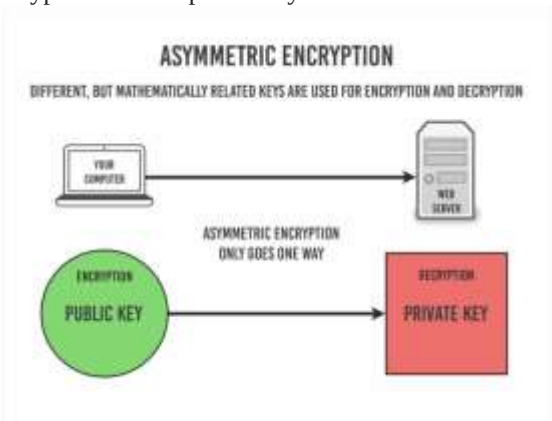

Figure 3 : Asymmetric Cryptography

1.3.3. Hash function

Hash functions, also called *message digests* and *one-way encryption*, and are algorithms that, in essence, use no key Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a mechanism to ensure the integrity of a file.

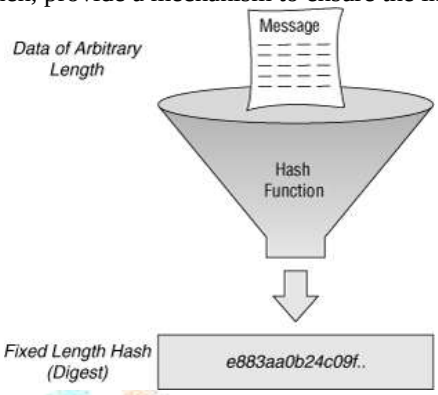

Figure 4 : Hash Function

1.4. Attacks

An **attack** is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an Asset. There are four types' attacks in database.

1.4.1 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. If this attack fails, the attacker moves to the next.

1.4.2 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.

1.4.3. Passive Attack: In this, 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.

1.4.4. Active Attacks: In active attack, actual database values are modified. These are more problematic than passive attacks because they can misguide a user. 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.

1.5. DBMS

A database-management system (DBMS) is a computer-software application that interacts with end-users, other applications, and the database itself to capture and analyze data. A general-purpose DBMS allows the definition, creation, querying, update, and administration of databases.

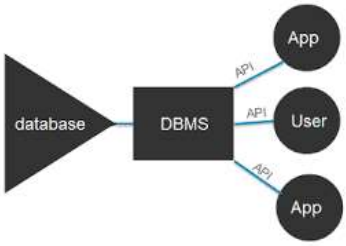

Figure 5 : DBMS

1.6. Threats

Threats are potentials for vulnerabilities to turn into attacks on computer systems, networks, and more. They can put individuals' computer systems and business computers at risk, so vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage.

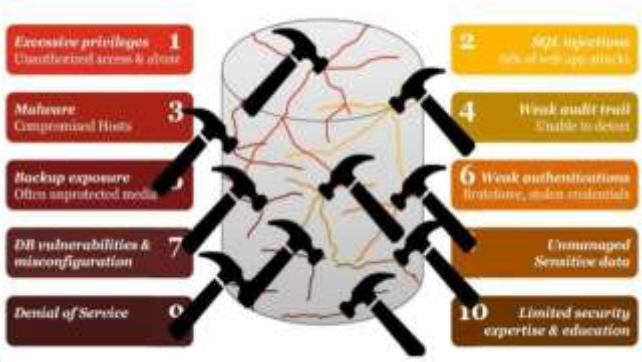

Figure 6 : Threats in Database

Threats to security in Database

1.6.1. Excessive privileges

When database users are granted enormous allowance that exceeds then their required job function, than these privileges may be abused for malicious purpose. E.g. a user in a company have the rights to change employee contact information may take advantage of excessive database update privileges to change salary information.

1.6.2. Legitimate Privilege Abuse

Legitimate privilege abuse is when an authorized user mistreats their legitimate database privileges for illegal purposes. Legitimate privilege abuse comes in existence when the database administrators or a system manager misused their rights and doing any unconstitutional or unethical activity. But this threat is not bound to, any misuse of sensitive data or unjustified use of privileges.

1.6.3. Privilege Elevation

Sometimes there are errors in software and attackers can take it as a chance to convert their access rights from normal user to those of an administrator, which could result in fake accounts, funds transfer, and misunderstanding of certain analytical information.

1.6.4. Platform Vulnerabilities

Vulnerabilities in operating systems such as window 98, window 2000 etc. and additional services installed on a database server may lead to illegal access, denial of service or corruption of data. E.g., the Blaster Worm which is a type of computer worm that spread on Windows 2000 vulnerability to construct denial of service conditions.

1.6.5. SQL Injection

In this attack, an attacker execute (or "injects") random unauthorized SQL statements into a liable SQL data channel. Targeted data channels consists stored procedures and Web application input parameters. Inserted statements are then passed to the database where they are executed.

1.6.6. Weak Audit Trails

A database audit policy assures automated, on time and appropriate tracking of transactions performed in database. This kind of feature must be a part of the database security policy since all the crucial database transactions have an automated record and if it is missing in it may causes serious risk to the organization's databases and could results instability in working.

1.6.7. Denial of Service

This type of attack prohibit the all legitimate users of a database to access some specific service in database. Attacker may crash the server by getting access to the databases. There are various conditions of DOS which may be created via many techniques like data corruption and network flooding etc.

1.6.8. Backup Data Exposure

Backup database storage media is often not safe from an attack and exposure to high risk as well as a natural disaster like flood, earthquake etc. As a result, many high profile security breaches have involved theft of database backup tapes and hard disks.

II. Literature Review/Related work

In this area significant amount of work is found. Here we have reviewed and used following references for this article.

2.1. Shelly Rohilla, Pradeep Kumar Mittal

Databases are a favorite target for attackers because of their confidential and important data. There are many ways in which a database can be compromised. There are various types of attacks and threats from which a database should be protected. In this paper, solutions of most of the threats mentioned, although some solutions are good while some are only temporary. Different types of threats are discussed in this paper

2.2. Shivnandan Singh, Rakesh Kumar Rai

Databases form the backbone of many applications today. They are the primary form of storage for many organizations. So 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.

2.3. Mubina Malik, Trisha Patel

Data is stored in database for easy and efficient way to manage these data. All the operations of data manipulation and maintenance are done using Database Management System. Considering the importance of data in organization, it is absolutely essential to secure the data present in the database. A secure database is the one which is reciprocated from different possible database attacks. Security models are required to develop for databases. Different types of control methods discussed in this paper.

III. Conclusion

Any organization, data is a most valuable property. Security of sensitive data is always a big challenge for an organization at many levels. In today's digital world, database is vulnerable to hosts of attacks and risks. In this study major security issues faced databases are identified and some control methods are discussed that can help to reduce the attacks risks and protect the sensitive data and information. It has been concluded that control methods provides confidentiality but give no assurance of integrity unless we use some digital signature or Hash function. Using strong cryptography algorithms reduces the performance. The future work could be carried out make cryptography more effective and efficient.

IV. Acknowledgment

We take this opportunity to thank our teachers for their support and encouragement for completing this report. Without their willingness to help us, this could not have been an easy task to complete.

V. References

1. Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.
2. Shivnandan Singh, Rakesh Kumar Rai, A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.
3. Mubina Malik, Trisha Patel, Database Security- Attacks and Control Methods. International Journal Information Sciences and Techniques, Vol. 6 (1/2) , 2016.
4. Deepika, Nitasha Soni, and Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.
5. Debasish Das, Utpal Sharma & D.K. Bhattacharyya, An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications, Volume 1, 2010.
6. Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009.