International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016

DATABASE SECURITY - ATTACKS AND CONTROL METHODS

Mubina Malik[1] and Trisha Patel[2]

CMPICA, Charotar University of Science & Technology (CHARUSAT), Changa

ABSTRACT

In today's world, data is generated at a very rapid speed and final destination of such data is database. 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. These models are different in many aspects as they are dealing with different issues of the database security. They may different also because of they are taking different assumptions about what constitutes a secure database. So, it becomes very difficult for database security seekers to select appropriate model for securing their database. In this paper, we have discussed some of the attacks that can be possible with its counter measures and its control methods that can be possible. Securing database is important approach for the planning of explicit and directive based database security requirements. Ensuring security for database is very critical issues for the companies. As complexity of database increases, we may tend to have more complex security issues of database.

KEYWORDS

Security, Threats, Attacks, Database, DBMS

1. INTRODUCTION

A database can be defined as a collection of data that is saved on a computer system's hard drive. Databases allow any authorized user to access, enter and analyse data quickly and easily. It's a collection of queries, tables and views. The data stored in the databases are usually organised to model aspects that support processes that require information storage and retrieval. Major chunk of data are stored in the repository called database [1]. The user interface for databases is called a database management system. DBMS are a software application that interacts with the authorised user, other applications and the database itself to capture and analyse data. It helps to organize data for better performance and faster retrieval by maintaining indices.

DBMS performs the function of concurrency control. DBMS also performs data recovery operations of database [1]. Now a day's Enterprises need databases to store any type of data needed, because of the speed and affordable cost database is popular among the enterprises. Advantage of using the database is it automates different procedures, saving resources and man hours. For example, instead of manually verifying transactions, users can rely on computer reports stored in the database. Instead of entering warehouse or retail stock information manually, Hand held scanners can be used to save information in the database. A database can provide efficiency and speed in the modern workplace. Next question for any organization is "Is Data secured using database?" Security in today's world is one of the important and challenging tasks that people are facing all over the world in every aspect of their lives. Databases are complex and many database security professionals do not have full understanding of risk and security issues related to different databases. According to many IT experts and DBAS, many enterprise DBAS

DOI : 10.5121/ijist.2016.6218

are not aware of which databases, tables and columns contain sensitive data because they are either handling legacy applications or there are no records or documentation of the data models. Even with full knowledge of the database assets databases are harder to secure because there are unique implementation and procedure for databases. We can say that database security is the use of a wide range of data security controls to protect databases against any attacks (internal or external), against compromises of database confidentiality, integrity and availability. The security involves different types of controls like technical, administrative and physical controls. Similarly security in electronic world has a great significance. Protecting the confidential/sensitive data stored in a repository is actually the database security [2]. There are various security layers in a database. These layers are: database administrator system administrator, security officer, developers and employee [2] and security can be breached at any of these layers by an attacker [5].

2. LITERATURE REVIEW

A Significant amount of work is found in this area. Here we have reviewed and used following references for this article.

Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin

It is concluded that databases is the backbone for any type of applications. Database contains very important and confidential information so there is a chance of attacks. 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 are discussed. Even some future research areas in the field of database security are also discussed in this paper.

Mr. Sohail IMRAN, Dr. Irfan Hyder

In this paper, author had discussed different security issues and its models for different types of database management system. Several proposals for discretionary and mandatory security models for the protection of conventional databases and object-oriented database systems are presented. Still, there is not a standard for designing these security models. The work presented in this paper gives a collected picture of different security issues of database; it can be extended to define, design and implement an effective security policy on a database environment and provides a consolidated view of database security.

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.

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. Review of some important database security techniques like

access control, techniques against SQLIA, encryption and data scrambling are discussed. 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.

3. DATABASE THREATS

Databases today are facing different kind of attacks. Before describing the techniques to secure databases, it is preferable to describe the attacks which can be performed on the databases. The major attacks on databases can be categorized as shown in Figure. 1. These attacks are further elaborated in the following sections.

3.1. Excessive privileges

Privileges of database can be abused in many ways. User may abuse privilege for unauthorized purpose. Privilege abuse comes in different flavours: Excessive privilege abuse, legitimate privileges abuse and unused privilege abuse. This type of threat is most dangerous because authorized users are doing misuse of data. These privileges can be abused and creates unnecessary risk.

Granting excessive permissions is problematic for two reasons. About 80% of the attacks on company data are actually executed by employees or ex-employees. Granting too many privileges or not revoking those privileges in time makes it unnecessarily simple for them to execute their wrongdoing. Some of these actions might even be executed inadvertently or without the perception of those actions being illegal

Abuse of legitimate privileges can be considered database vulnerability, if the malicious user misuses their database access privileges.

Countermeasures of Privilege Abuse include

1. Access Control policy: Do not grant unnecessary privileges to the user.

2. Legitimate privilege abuse can be stop by a providing good audit trail.

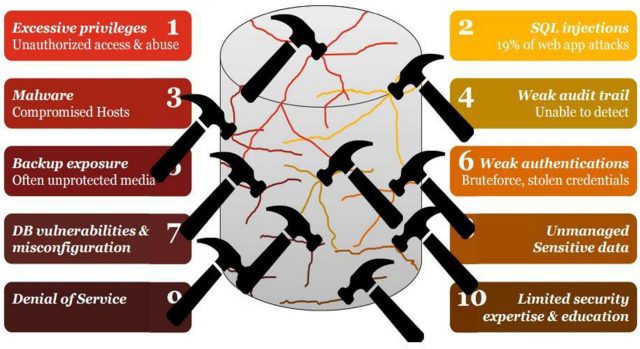

Figure 1. Database Threats

3.2. SQL Injections

Database systems are used for the backend functionality. User supplied data as input is often used to dynamically build sql statements that affect directly to the databases. Input injection is an attack that is aimed at subverting the original intent of the application by submitting attacker – supplied sql statements directly to the backend database.

There are two types of input injection:

1. SQL Injection
2. NoSQL Injection.

SQL Injection: Targets the tradition database system. It attacks usually involve injecting unauthorized statements into the input fields of applications.

NoSQL Injection: Targets big data platforms. This type involves inserting malicious statements into big data components like Hive, MapReduce.

In SQL and NoSQL successful input injection attack can give attacker unrestricted access to an entire database.

Countermeasures of Input Injection

1. Use Stored Procedure instead of implementing direct queries.
2. Implementing MVC Architecture.

3.3. Malware

Cybercriminals, state-sponsored hackers, and spies use advanced attacks that blend multiple tactics – such as spear phishing emails and malware – to penetrate organizations and steal sensitive data. Unaware that malware has infected their device; legitimate users become a conduit for these groups to access your networks and sensitive data.

Countermeasures of Malware

Enable firewall protection and Install Antivirus.

3.4. Weak Audit Trail

Weak audit policy and technology represent risks in terms of compliance, deterrence, detection, forensics and recovery.

Automated recording of database transactions involving sensitive data should be part of any database deployment. Failure to collect detailed audit records of database activity represents a serious organizational risk on many levels. Organizations with weak database audit mechanisms will increasingly find that they are at odds with industry and government regulatory requirements. Most audit mechanisms have no awareness of who the end user is because all activity is associated with the web application account name. Reporting, visibility, and forensic analysis are hampered because there is no link to the responsible user. Finally, users with administrative access to the database, either legitimately or maliciously obtained, can turn off native database auditing to hide fraudulent activity. Audit capabilities and responsibilities should ideally be separate from both database administrators and the database server platform to ensure strong separation of duties policies.

Countermeasures of Weak Audit Trail

1. Network-based audit appliances are a good solution. Such appliances should have no impact on database performance, operate independently of all users and offer granular data collection.

3.5. Backup Exposure

Backup storage media is often completely unprotected from attack. As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect backup copies of sensitive data and monitor your most highly privileged users is not only a data security best practice, but also mandated by many regulations.

Countermeasures of Backup Exposure

1. Encrypt Databases: Store data in Encrypted form as this allows you to secure both production and backup copies of databases, then audit the activity of and control access to sensitive data from users who access databases at the operating system and storage tiers. By leveraging database auditing along with encryption, organizations can monitor and control users both inside and outside of the database.

3.6. Weak Authentication

Weak authentication schemes allow attackers to assume the identity of legitimate database users. Specific attack strategies include brute force attacks, social engineering, and so on. Implementation of passwords or two-factor authentication is a must. For scalability and ease-of-use, authentication mechanisms should be integrated with enterprise directory/user management infrastructures.

3.7. DB Vulnerabilities and Misconfiguration

It is common to find vulnerable and un-patched databases, or discover databases that still have default accounts and configuration parameters. Attackers know how to exploit these vulnerabilities to launch attacks against your organization. Unfortunately, organizations often struggle to stay on top of maintaining database configurations even when patches are available. Typical issues include high workloads and mounting backlogs for the associated database administrators, complex and time-consuming requirements for testing patches, and the challenge of finding a maintenance window to take down and work on what is often classified as a business-critical system. The net result is that it generally takes organizations months to patch databases, during which time they remain vulnerable.

Countermeasures of Misconfigured Databases

1. No default accounts should be there. Accounts must be created using fresh username and password.

3.8. Unmanaged Sensitive Data

Many companies struggle to maintain an accurate inventory of their databases and the critical data objects contained within them. Forgotten databases may contain sensitive information, and

new databases can emerge – e.g., in application testing environments – without visibility to the security team. Sensitive data in these databases will be exposed to threats if the required controls and Permissions are not implemented.

Countermeasures of unmanaged Sensitive Data

1. Encrypt Sensitive data in Database.

2. Apply required controls and Permissions to the database.

3.9. Denial of Service

Denial of Service is a general attack category in which access to network applications or data is denied to intend user.

Countermeasures of Denial of Service

1. Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.

2. Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

3.10. Limited Security Expertise and Education

Non technical security is also play an important role. Internal security controls are not keeping pace with data growth and many organizations are ill-equipped to deal with a security breach. Often this is due to the lack of expertise required to implement security controls, enforce policies, or conduct incident response processes.

Countermeasures of Limited Security and Education

1. User Education and awareness
2. Cultivate Experience Security professional.

4. CONTROL METHODS FOR DATABASE THREATS

To remove the security threats every organization must consists a security policy which should be implemented for sure. In security policy authentication plays a vital role because if authentication is proper than there is less chances of threats. Different users have different access rights on different database objects. Access Control Mechanisms deal with managing the access rights. It is the basic technique to protect the data objects in the databases and is supported by most of the DBMS [6]. Figure 2 gives the overview of the control methods used for database security.

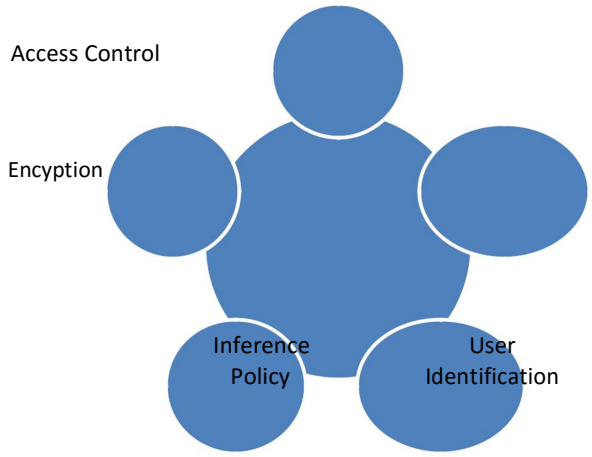

Figure 2. Control Methods

4.1. Access Control

Access control is one of the fundamental services that any Data Management System should provide. Its protected data from unauthorized read and write operations. Access control define make sure that all communication to the database and other system objects are strictly follow the policies. Errors can be as major which can create problem in firm's operation. Through controlling access rights may also helps in reducing the risks that may precisely impact the security of the database on the main servers. For instance, if any table is deleted or access is modified accidently the results can be roll backed or for specific files, but through applying the access control their deletion can restrict.

Access Control systems include:

1. File permissions - create, read, edit or delete on a file server.
2. Program permissions - right to execute a program on an application server.
3. Data rights - right to retrieve or update information in a database.

4.2. Inference Policy

It is very essential to protect data at specific level. It can be applied when analysis of particular data in the form of facts are required to be prevented at a certain higher security level. It helps to determines how to protect information from being released.

The aim of the inference control is to avoid indirect disclosure of information. Generally there are three ways to unauthorized data disclosure:

1. Correlated data - typical channel when visible data X are semantically related with invisible data Y

2. Missing data - result of query contains NULL values that mask sensitive data. Existence of that data may by detect that way.

3. Statistical inference - typical for databases that provide statistical information about entities.

4.3. User Identification /Authentication

A basic security requirement is that you must know your users. You must identify them before you can determine their privileges and access rights, and so that you can audit their actions upon the data.

User can be authenticated in many ways before they are allowed to create database. Database authentication includes both identification and authentication of users. External authentication can be performed by the operating system or network service. Also the user authentication can be defined by Secure Socket Layer (SSL), through enterprise roles, through middle tier server authentication also known as proxy authentication.

This is the very basic requirement 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.

Attacker can take different approaches like bypass authentication, Default Password, privilege escalation, Password Guessing by brute force and rainbow attack when they attempt to compromise user identification and authentication [1].

4.4. Accountability and auditing

Auditing is the monitoring and recording of configured database actions, from both database users and non database users. Accounting is the process of maintaining an audit trail for user actions on the system. 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.

If a user has managed to authenticate successfully and tries to access a resource, both successful and unsuccessful attempts should be monitored by the system, and access attempts and their status should appear in the audit trail files.

4.5. 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.

There are two states for data protection in database. Data may exist either At Rest – data may be stored in a database or in backend tape or At Transit – Data travelling across the network which dictates different encryption solutions for the data in transit. Data encryption can solve some of the issues related to data At Rest. For Data at Transit needs leverage solutions such as SSL/TLS.

5. CONCLUSION

To summarize, access protection begins with who can access data and what type of data attackers want to access. There is a lot of scope to improve the techniques used for database security. According to the survey 84% companies feel that database security is adequate. 73% of companies that predict database attach will increasing day by day. 48% of attackers are authorized users. 48% of users have done misuse of their privileges. We have also discussed the

issues related to security database. Several proposals for discretionary and mandatory security models for the protection of conventional databases are presented. Still, there is not a standard for designing these security models. The work presented in this paper gives collected information of different threats and its security issues of database. It can be extended to define, design and implement an effective security policy on a database environment and provides a consolidated view of database security. According to the survey this paper focused on threats and its possible counter measures that can be possible to secure data in databases.

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] Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.

[3] Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009.

[4] Jiping Xiong, Lifeng Xuan, Jian Zhao and Tao Huang, Web and Database Security, Zhejiang Normal University.

[5] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[6] Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[7] 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.

[8] 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.

[9] 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 No.1–25,2010.