Security Of Database Management Systems

Article · January 2016

CITATIONS
3

READS
26,775

1 author:

Ashour A N Mostafa
The Higher Institute of Science and Technology - Tobruk
15 PUBLICATIONS **84** CITATIONS

Security of Relational Database Management System: Threats and Security Techniques

ASHOUR A N MOSTAFA / ID: 153915643

Infrastructure University Kuala Lumpur, Malaysia

Faculty of Creative Media and Innovative Technology

Abstract:

The history of database research backs to more than thirty years, in which created the concept of the relational database system that has become the most fundamental change for organizations strategy. Technology evolution has produced more powerful systems that relate to economic impacts in the recent decade.

Organizations must ensure its information and data be secured and confidential. Therefore, they deploy systems or applications have functions, services, and tools for data maintenance and management packed into the so-called Relational Database Management System (RDBMS). Such functions contain services plus privileges for authorization to keep legitimate users (authorized) to access the database. The database must be insecure. **RDBMS** refers to relational database management systems that are using a relational model that developed by the researcher Codd at IBM laboratory.

Database protection means disallowing illegitimate users to access the database and its sensitive information whether intentional or accidental [4]. Therefore, most of the firms are taking account of possibility of threats as measures to their database systems. This paper addresses the relational database threats and security techniques considerations in relation to situations: threats, countermeasures (computer-based controls) and database security methods [1, 8, 9].

Introduction:

As known, in recent years, hardware capability and capacity of volumes, in addition, huge uses of World Wide Web platforms and information systems have led to adopt the relational database systems as infrastructure to the data repository. Huge amounts of data and information has become prime concern of security challenges because the management of information has become decentralized.

CIA triangle of security that refers to confidentiality, integrity, and availability often is the basis of relational database security concept. These factors must be existed into application processes to guarantee the data to be in safe [1].

Theft and fraud have an influence on the database environment, and hence the whole corporation. It is not rather making changes on the data itself, but it may decrease the

privacy and integrity. Confidentiality refers to maintain the secrecy of data, usually only is critical to the organization. Breaches of security resulting in loss of confidentiality could lead to loss of privacy and competitiveness. Failure of integrity means the data is corrupt and modified.. Many organizations are seeking the availability, the so-called 24/7 availability (that is, 24 hours a day, 7 days a week). Loss of availability means the system, or the data, or both cannot be accessed. Therefore, relational database management system aims to reduce the losses that are caused by threats or anticipated events. Threat is a situation or an event that may adversely affect a system, and hence the organization. The organization should invest time and effort to detect and identify the most serious threats [1, 8, 9].

Millions of online operations conduct via unreliable Internet connection such as electronic commerce and electronic banking. Those types of transactions impose a kind of transferring sensitive assets and information [2]. This is a challenge to the services providers to get user's trust. Therefore, it has a strong protection of data containers such a RDBMS. Not all kind of data require being safe and protected, but the most critical data that relate to users' information and money transactions. Corporation can specify the nature of information needed to be encrypted with high level of security such as ministry of defense [8, 9].

This paper shows some of the countermeasures that are computer-control based such as authorization, access control, backup and recovery, encryption. It must taking account the encryption process of sensitive data require high performance of the system because it will need decrypting of those data. Therefore, the programmer must ensure using optimized security algorithms while coding the application [8, 9].

1. What are the Attacks?

Rapid evolution of breach methods to the SME organizations called to adopt standards of security measures like CIA. However, it becomes sophisticated due to diversity of attacks either direct or indirect.

The unclassified user can have legal access to the database to use public information, but he may be able to infer classified information. There are three levels of attacks to the relational databases: direct, indirect and by tracking. **Direct attack** is obvious. The attacker can easily access to the database if it does not have any protection mechanism. **Indirect attack** is used by expecting the desired data from displayed data using combinations of queries. The tracking attack is executed by suppression of the dominant results [3].

RDBMS threats can be summarized as:

- The administrator could be grant the user privileges that not required. Abuse of uses of these privileges may lead to create trapdoors of the application.
- The user has a legitimate privilege access to the database. He/She may have bad intention to abuse the utility.

- One of the threats is vulnerability of the software or the operating system. This helps the intruder to breach sensitive information as backdoors.

1.1. Mechanisms of Attack Control [3]:

- Rejection without any response when the requests for accessing the database to display the results of sensitive data.
- Disability of the intruder to guess the real information or values because the system will display the results close to the real ones.
- When the sensitive data will be detected, the system should limit the results to prevent the attacker to reveal the data.
- Combination of the results will make the attacker to be confused about knowing the sensitive data.

2. Countermeasures (Computer-based Control):

This type ranges from physical controls to administrative procedures. It can be categorized into various forms of control as [1]:

- Authorization.
- Access controls
- Views.
- Process of Backup.
- Integrity.

Authorization is granting process of a right or privilege to a subject (a user or a program) to have legitimate access to a system or systems' objects. It involves the authentication of subject requesting access to objects. The administrator usually create accounts with specific privileges according to the security level of the user.

Access Controls into a relational database can allow/disallow the user to access the system. RDBMS keeps track the privileges process.

Views are consequence of flexible operations were being conducted on the main relation. It is a mechanism of dynamic processes of security, in which it shows parts and hide other parts according to the users' privileges.

Process of Backup As known, the backup means capturing a copy of log files of instance processes plus a copy of the relational database periodically and storing either on external storage or cloud to restore later.

Integrity is a process to maintain a secure RDBMS by preventing data from becoming invalid, and hence misleading or incorrect results.

3. Techniques of RDBMS Security:

Encryption is encoding process of sensitive data to become unreadable. Most of relational database management systems support this purpose to secure its data [4].

The encryption concept has four main factors that are defined as [5]:

- An **encryption key** to encrypt the data (plaintext).
- An **encryption algorithm** with the encryption key transforms the plaintext to cipher text.
- A **decryption key** to decrypt the cipher text.
- A **decryption algorithm** with the decryption key transforms the cipher text back into the plaintext.

Two forms of encryption techniques that called symmetric and asymmetric. The symmetric one depends on the safe channel while exchanging the key, in addition, the key of encryption is similar to the key of decryption that is being utilized, for instance, IDEA (international data encryption algorithm) [6, 7]. Symmetric algorithm is much faster than the asymmetric algorithm that uses two different keys (private and public keys) such as RSA (the name is derived from Ron Rivest, Adi Shamir, and Leonard Adleman). Generally, they are often used together, in which public key (asymmetric) encrypts a randomly generated encryption key, and the random key encrypts the actual message (using a symmetric algorithm). The database scheme of encryption should enhance sharing of data within the database without losing data privacy [2, 6-9].

To improve the performance, the data should be divided into sensitive data and insensitive data. The insensitive data can be retrieved rapidly, and the sensitive data is encrypted/ decrypted using Encryption algorithms.

Web-based database security: the transmitted data from a server to a client must be in a secured way. The client should be authenticated such as **Host Identity Protocol (HIP)**. It sets up a trusted relationship between hosts on the Internet by passing to the web server. The HIP and Web server help in authentication process [2].

Log file is an important file to monitor the processes and operations occurred online. It periodically tracks the status of operations to indicate the modification may occur when the system fails. It also integrates with the audit module to track the log file of the users to guarantee the web database security [1].

Negative Database: this process depends on adding false data to the original to make the malicious users to be confused, and only valid to legal users. It has four modules: database cache, database encryption algorithm, virtual database, and negative database conversion. The first three generates the data for the conversion to generate false data [2].

4. How to develop a relational database encryption strategy?

It is a mechanism of increasing the strength of the data protection. Many factors to get strong encryption into RDBMS:

- The encryption should be implemented on the database or the application.
- The accessing to the encryption key.
- The amount of data that should be encrypted.

- Is there any influencing on the performance?
- For the programmer and the developer most of the responsibilities through creating or developing the database management system.

The programmers should be aware from creating trapdoors that can be formed through setting the policies and procedures.

Two strategies for encrypting the database and both have advantages and disadvantages:

- Encryption the RDBMS.
- Performing the encryption outside the database.

1. **Fundamentals of Encryption:**
   Algorithm and key size are factors to encrypt data within RDBMS. Administrator of the application may grant legitimate access to authorized users for need.

2. **Data encryption effect on RDBMS:**
   Encrypting the data needs high process operations. This drives to increase the size of RDBMS, then deceasing the utility or the performance. Consequently, sensitive data must be encrypted.

3. **Data stream into the application:**
   Data usually flows over Internet and an internal network. Therefore, the potential of risk is high.

4. **The key management:**
   It relates to how to manage the key that is used into RDBMS in terms of number of keys, the location of keys and the protection of the accessing of the encrypted keys.

4.1. Solutions of implementing encryption:

i. Inside the Relational Database Management System (RDBMS):

It is a simple way using the encryption/decryption method by RDBMS. It is a transparent to the application. When the data inserts inside the RDBMS, the data will be encrypted, or decrypted to the original when display.
A disadvantage of encryption inside the RDBMS is an extra processing load and decreasing in performance.

ii. Outside the Relational Database Management System (RDBMS):

Using the client/server security protocol (SSL) helps the data to be encrypted in the application whether in the source or to the destination.
The protection differs from application to another.
The solution is using the **Encryption Server** to provide a centralized encryption services for the whole database. The drawbacks include communication overhead, administering more servers and changing the applications.

Conclusion:

This report is to explain different methods of database security. Database risks are increasing by the risks of disclosure data. The programmers of RDBMS have responsibilities to increase and improve the security techniques of the databases without affecting on the performance. In addition, the user has responsibilities especially the ethics of using the sensitive data. We have described the types of Attacks and threat that the database could face them. Then, it has explained some mechanisms of attack control. It has explained about the countermeasures that are computer-based and has concentrated on the encryption method. In the same approach, it has described the database security techniques or method. The last part is about the benefits and drawbacks of using either encryption inside RDBMS or outer.

References:

[1] T.Connolly, C. Begg. "Database Systems
A Practical Approach to Design, Implementation, and Management", 4th ed., Ed. England: Person Education Limited, 2005, pp. 542-547, 550-551.

[2] Burtescu, E. (2009). Database Security-Attacks and Control Methods. *Journal of Applied Quantitative Methods*, *4*(4), 449-454.

[3] Kayarkar, H. (2012). Classification of Various Security Techniques in Databases and their Comparative Analysis. *arXiv preprint arXiv:1206.4124*.

[4] Kahate, A. (2013). *Cryptography and network security*. Tata McGraw-Hill Education.

[5] Stallings, W., & Brown, L. (2008). Computer security. *Principles and Practice*.

[6] Shaefer, E. F. (1996). A Simplified Data Encryption Standard Algorithm. Journal of Cryptologia, 20 (1), 77-84.

[7] Chang, H. S. (2004). *International Data Encryption Algorithm*. Retrieved from http://scholar.googleusercontent.com/scholar?q=cache:WXJPT0eEM7EJ:scholar.google.com/+International+Data+Encryption+Algorithm&hl=en&as_sdt=0,5 on 15 February 2013.

[8] Almasri, O., & Jani, H. M. Introducing an Encryption Algorithm based on IDEA.

[9] Almasri, O., Jani, H. M., Ibrahim, Z., & Zughoul, O. (2013). Improving Security Measures of E-Learning Database. *International Organization of Scientific Research-Journal of Computer Engineering (IOSR-JCE)*, *10*(4), 55-62.