Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security in Database Systems

By Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili

King Saud University

Abstract - The paper focuses on security issues that are associated with the database system that are often used by many firms in their operations. The rapid development and proliferation of Information technology has offered many opportunities for integrated business operations. It has enabled business enhances their efficiency and effectiveness in operations such as customer care, sales, human resources and production. However, these developments have served to bring issues of security. Many firms are falling victims of cyber crimes. These are malicious people who target their data and compromise its integrity. This is occasioned by unauthorized access, which makes data lose its integrity and lastly operations of the business are affected negatively. This paper will tackle various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.

Keywords : *database security, security techniques, database threats, integrity.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

Security in Database Systems

Abdulrahman Hamed Almutairi [α] & Abdulrahman Helal Alruwaili [α]

Abstract - The paper focuses on security issues that are associated with the database system that are often used by many firms in their operations. The rapid development and proliferation of Information technology has offered many opportunities for integrated business operations. It has enabled business enhances their efficiency and effectiveness in operations such as customer care, sales, human resources and production. However, these developments have served to bring issues of security. Many firms are falling victims of cyber crimes. These are malicious people who target their data and compromise its integrity. This is occasioned by unauthorized access, which makes data lose its integrity and lastly operations of the business are affected negatively. This paper will tackle various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.

Keywords : database security, security techniques, database threats, integrity.

I. Introduction

Sorting Database security is a crucial operation that a firm should enhance in order to run its activities smoothly. It is a deliberate effort to protect an organization data against threats such as accidental or intentional loss destruction or misuse. The threats pose a challenge to the organization in terms of integrity of the data and access. The threat can result from intangible loss such as hardware theft or intangible loss such as loss of confidence in the organization activities. All these activities have been rampant due to electronic commerce as opposed to convectional trade involving physical goods. There has seen consumers been sensitive to any cases of security violations. It is also very hard to apprehend culprits who commit the violations because of the remoteness of transactions. Also, most database store sensitive information for consumers which can be vulnerable to hacking and misuse. Therefore, firms have embraced greater controls and checks on their database to maintain the integrity of the information and ensure that their system are monitored closely to avoid deliberate violations by intruders.

II. Threats of Database Security

Database security issues have been more complex due to widespread use and use of distributed client/server architecture as opposed to mainframes system. Databases are a firm main resource and therefore, policies and procedure must be put into place to safeguard its security and the integrity of the data it contains. Besides, access to the database has been become more rampant due to the internet and intranets therefore, increasing the risks of unauthorized access (Singh, 2009).

The objective of database security is to protect database from accidental or intentional los. These threats pose a risk on the integrity of the data and its reliability. Besides, database security allows or refuses users from performing actions on the database. Database managers in an organization identify threats and make policies that take action to mitigate any risks. Such actions include controls using passwords and username to control users who access the databases. The system created is called database management security system which keeps user details and allows access when provided with passwords and usernames (Singh, 2009).

There are different threats to the database systems. Loss of availability means that data or systems cannot be accessed by any user. This most often arise from sabotage of the hardware, applications or networks system. This may halt the activities of the organization as well impede on the operation in the day to day activities of the organization (Singh, 2009). For example, in case of a bank where customers can looses their confidence in the security of their deposits and eventually the bank lose customer and performance decline. Excessive privilege abuse is another method through which data can loss its integrity. When users are given too much privilege in the system database they abuse them for malicious purposes. For example, in the accounting department, the user may change other issue not concerned with the function of his job. All privileges should match the job requirements for each user (Singh, 2010).

Another threat to database security is that of privileges elevation. This is when some user can convert extra privileges from ordinary user to administrator through taking database platform software vulnerability. For example, in a firm accounting department, a user may convert excess rights to that of administrator and use them to create illegal transactions and accounts. This is done by exploiting the software weaknesses in the database system (Singh, 2009).

Another threat is having a weal audit trial. This is when an organization exposes itself to risk of various types due to weaknesses in its internal system. This is due to weak deterrence mechanism. Denial of service is another problem in database security. This is a kind of

Author α : King Saud University, College of computer and information sciences.

an attack where data or network applications are targeted to avoid access to users. Often, the intention is to extort money. For example, attackers can crash servers from remote areas and then extort money. Other techniques that can be used in denial of service include data corruption, network flooding and resource overload.

Another threat to the problem of database insecurity is weak system and procedures for performing authentication. Weak authentication can result to attackers getting legitimate rights of user and then steal or change credentials. Some of the ways in which an attacker can hack in include use of social engineering, where passwords are requested through phone calls for maintenance purposes. Other include brute force where the attacker does guess the passwords. Strong authentication is therefore required to address these challenges. Besides that, there is backup data exposure, where the storage media is left exposed leading to attacks. For example, tape and hard disks need to be secured well (Singh, 2009).

Loss of data integrity can cause the data to be corrupted and invalid. This can results to delay in operations of the company as well as making wrong decisions which can affect the performance of the company (Singh, 2009). This can only be restored through backup and recovery procedures. Another issue at player is the loss of confidentiality. This is where the secrecy of crucial data in an organization is breached resulting to loss of confidentiality and eventual loss of competitiveness (Singh, 2009). Another threat to database system is the loss of privacy. This can lead to the firm being subjected to blackmail, bribery and shame.

Theft or fraud is also common in firms such as banks. This occurs when personnel enter protected areas where databases are hosted and interfere with the systems. To prevent this threat, the firms should have controls on restricted areas as well install firewall to prevent people gaining unauthorized access to the database systems (Singh, 2009). Other threats that can be detected are accidental losses which could result from malfunctioning systems and operating procedures. Other forms of threats to databases could include inference theft. This is the process of sending queries deducing unauthorized information from legitimate sources. Identity theft is another form of threat to database. This is the situation where a person poses as another person and uses social security number to wipe out the details of the holders (Kumar, 2005).

There are several goals that are often targeted for database security issues. The first one is confidentiality. This relates to secrecy or privacy in terms of access by authorized subjects or processes.

The second goal is to ensure that integrity is maintained and that means that data can only be changed by authorized subjects. Another goal is the availability of data. This is the need to maintain access to only authorized persons.

III. Security Threat Classification

Several Human errors can be said to be accidental in that incorrect input and wrong use of applications can be seen as a factor that can lead to such threats. Errors in software include those of incorrect applications of security protocol and denial of access to authorized users. Natural or accidental disasters can also be cited as one of the factors of security concerns. This includes damage of software and hardware (Kumar, 2005).

IV. Classification of Database Security

Security of databases involves restoring the database to a safe mode after failure. There are various types of security issues that are related to database. Physically security can be said to be security of the hardware associated with the system and where the database is hosted or located. Some cause such as floods and earthquakes can be a threat to that and the only solution is to store databases back up. The other types of measure are the system issues or logical security. These are measures that resides in the operating systems and usually far more difficult to achieve (Sumathi, 2007).

V. Guidelines for Database Security

For some steps need to be taken in order to build a robust system. This is a system which has got Simplicity in design and very easy to use and that make it less vulnerable to attacks. Normalization of the database should be done at early stages before use to enhance its functioning and avoid hitches after updates. Allocation of privileges to different users is another guide in that each user should be allocated some privileges to avoid chances of hacking. It is also important for users to create view for each group of users. After the designing stage, the database needs to be maintained and several issues needs to be taken care of. There are some procedures that need to be taken care of in maintenance. The first one is operating systems issues and availability.

Operating system should be capable of ensuring verification of users and applications programs which attempts to access the system and authorizes them. This work is handled by the database administrator who also keeps accounts and passwords (Sumathi, 2007).Besides that there is confidentiality and accountability. By accountability, the system should not allow any user without its permission to avoid illegal access. Therefore, there is need to monitor authentication and authorization of users. Authorization is usually handled by controls which are found on the database management system that controls access by

users and actions done when accessing the database. Authentication is usually carried out operating system. The database administrator creates passwords for every user (Sumathi, 2007). The next step is through encryption. This is defined as coding of data so that it is not read and understood easily by the users. Database management system have system to encode data which is extremely sensitive for transmission over channels. It also provides a channel for decoding data which is also secured enough (Sumathi, 2007). Database system have also a mechanism to verify whether what the user claims to be is actually true. Such measure include passwords and usernames that enable the authentication of users. It is hosted at the operating system or at the database system management system. Passwords are legitimate user access methods.

VI. Process of Creating Database Architecture

We Security in database can be enhanced through a process of developing architecture system. There is a process of maintaining and establishing security architecture. The first phrase according to Basta and Zgola 2010 is carrying out assessment and analysis. This involves identifying the security threats, vulnerability and resources that exist in the devices and vendor partnership. A through and exhaustive audit of the database environment should be done. This is to identify any social engineering gaps as well firewall faults. Experts are normally called in to identify risks, define the likelihood of a threat of an asset and determine the cost of any such threat to the assets. Once this is done, the next step is to come up measure to counteract these threats.

The next phrase is to design and model the system. This is usually done through creating policies and prototype security that satisfies the business needs. AT this stage, policies and procedures are created and the software is defined. Once this is done, the next step is to identify tools and applications for reducing risks (Basta and Zgola 2010).

The third stage is usually deployment. This is the phase where the tools firewall and applications are put into place. The exercise involves making simulation in terms of deployment tests. These are simulation tests that helps to test the robustness and any case of unforeseen variable do affect overall security objectives (Basta and Zgola, 2010).

The fourth stage is the management and support. This is where the ongoing support and assessment of the security architecture was deployed as seen in the previous phase Monitoring is done to ensure that changes can be rectified as soon as possible. Need for reassessment and initiating the start of security life cycle (Basta and Zgola 2011).

VII. Illustration of Maintaining and Creating Database Security Architecture

Figure 1 : Database Security Architecture

VIII. Techniques for Database Security

Authorization can be one of the techniques that can be used for granting rights of access of a subject into a system. Another method that is effective is the view. This is a virtual table that can be produced at the time of request of data access. What happens is that view has to have access in the tables other than the base tables in such a way those restrictions are made on the user. This provides appropriate security to crucial data.

Back up is the process of taking to an offline storage facility, data and log file. To keep track of transaction involving the database, it is necessary for one to have journal file on all updates of the database. In event of failure of the database system, the log file and the database are then used to restore the database to normal functioning position. Integrity constraint is used to contribute to avoid cases of data becoming invalid and hence giving misleading information. The ultimate goal of the constraints is to maintain integrity of the data and hence its consistency. Database can be secured through encryption. This is encoding of the system using special algorithm that is only accessible when decryption key is provided. This is especial useful when sending sensitive information over communication lines (Bertino et al (2005).

Audit trial is another method that can help in the database security. Audit trial need to be carried to found the history of operations on the database. It is necessary to restore information lost as well as discover abuse of privileges by any users (Singh, 2009).

Another technique that can be used to secure database is the use of access control. This is the where the access to the system is only given after verifying the credentials of the user and only after such verification is done, the access is given. Use of steganography is rampant in the era of information technology. This technique is used to hide information from unauthorized access. What happens is the data is embedded in the LSB's of the pixel value. Certain number bits are used to hide sensitive information (Basta and Zgola, 2011).

IX. Various Techniques for Database Security

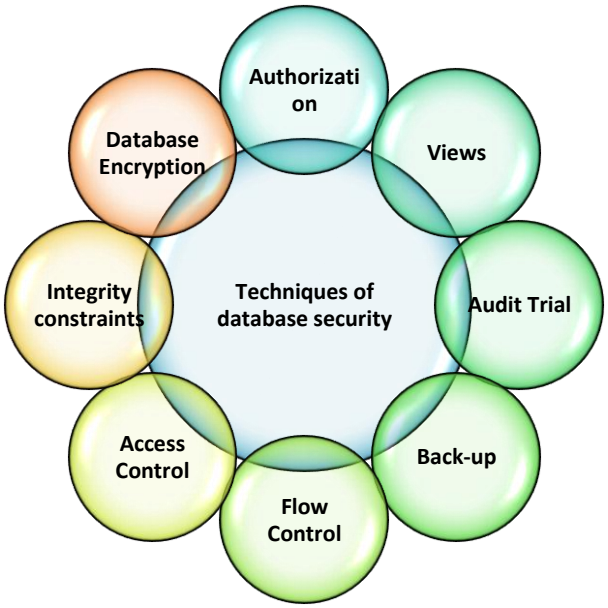

Figure 2 : Various techniques for database security

X. Advantages of Database Management System

What A database management system is used is a group of programs that manages the database structure and controls the access to the data stored in the database. It is thus an intermediary of between the users and the database. It has several advantages. It improves data sharing in a way that enables the end users have better access to data that is correctly managed. There is improved data security in that the security is guaranteed and the data privacy is maintained. Database management has an effect of ensuring that there is promotion of data integration in a whole organization and one can see a bigger picture of all activities (Coronel et al, 2012). There is also minimized data inconsistency such that the anomalies such as storing different data in different places is reduced. It is also probable that data access is facilitated and could be used to provide quick answers to queries giving out. There is better decision making is achieved due to accuracy, timelessness and validity of the information generated. The final result is increased end user productivity because it empowers one to make rational decisions for the success of the business (Coronel et al, 2012).

XI. Requirements for Database Security

User authentication and identification is normally required before the user can access the database. Authentification methods are passwords, biometric readers or signature analysis devices. These are required for better management of users. The second requirements involves authorization and access controls. These are the rules that govern what access to what information. These policies govern how information is disclosed and then modified. When you look at the access controls, these are the polices that govern the authorizations. There has to be integrity and consistency in the database operations. There has to be a correct set of rules in operation which protects the database from malicious destructions. Auditing is another requirement in database. This demands that a record of actions pertaining to operations. This is necessary in order to review and exams the efficiency of the controls system and recommend for better actions (Coronel et al, 2012).

XII. Integrity Principles in Database Security

Answers Data integrity refers to reliability and accuracy of the data that is stored and used in business. Data should assist a firm to make the right decision and avoid inconsistencies. Therefore, there are several guidelines that normally should be adhered to. The first one is well-formed transactions. This means that data should not be liable to manipulation easily and arbitrarily by users. This promotes its integrity. This reduces chances of compromising on the data accuracy. It is paramount the privileges are given at minimum basics to restrict any unauthorized access. There must be a separation of duties in that, individual should be exposed to misuse assets on their own. In database security, there must be ability to reconstruct events such that it is possible to hold individual accountable for their actions. Every organization has a structure and this structure has people who are charged with the responsibility to delegate authority. Another principle is that there must be continuity of operations. This means that, in face of calamity such as disaster, the operations of the firm must continue at some degree (Coronel etal, 2012).

Figure 3 : Database security

XIII. Conclusion

Which the paper has generally discussed the database security concerns and research into various issues surrounding the sector. Organizations now are relying on data to make decisions on various businesses operations that enhance their operations. Therefore, it is prudent to keep sensitive information away from unauthorized access. Database security research paper has attempted to explore the issues of threats that may be poised to database system. These include loss of confidentiality plus loss of integrity. Besides, it has detailed on loss of privacy leading to blackmail and embarrassment in the business. The paper has also discussed areas concerning techniques to counter any issue of threat. These could be use of views and authentication. Another method is through back-up method which ensures that the information is stored elsewhere and recovered in case of failure or attacks. The paper has also discussed the requirements that are set for a robust database management system. Some of the requirements are audit trial. Lastly, the paper has looked at the process for managing a database system and has discussed all the steps that need to be taken.

References Références Referencias

1. Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers, 2005.
2. S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
3. S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
4. P, Singh Database management system concept V.K (India) Enterprises, 2009
5. A. Basta, and M. Zgola, Database security Cengage Learning, 2011.
6. Coronel et al Database System Design, implementation and management Cengage Learning, 2012.
7. Bertino et al Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.

This page is intentionally left blank