Volume 5, Issue 5, MAY 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Database Security: Threats and Security Techniques

Deepika, Nitasha Soni
Department of Computer Science,
Lingaya's University, India

Abstract-- Data security is an emerging concern proved by an increase in the number of reported cases of loss of or exposure to sensitive data by some unauthorized sources. Security is a composed part in which it protects and secures the sensitive data or database management software from some unauthorized user or from malicious attacks. In this paper we will be presenting some of the common security techniques for the data that can be implemented in fortifying and strengthening the databases.

Keywords: SQL, DOS, DBMS

I. INTRODUCTION

Information or data is one of the most valuable assets in any organization. Mostly organizations like social, governmental, educational etc., have now programmed their information systems and other working functions. They have sustained the databases that contain the sensitive information. This is the reason why database security is a serious interest. In actual terms database security is to prevent the confidential data which is stored in repository. It concern with making database secure from any sort of illegal access or risk at any level. Database security requires permitting or prohibiting user actions on the database and the objects under it. Organizations functioning well have asked for the confidentiality of their database. They do not allow the illegitimate user to access their data/information. And they also claim the assurance that their data is protected from any malicious or unexpected differences. Insurance of data and its secrecy are the security focus. Properties of database security [1][2][3] shown in Figure 1:

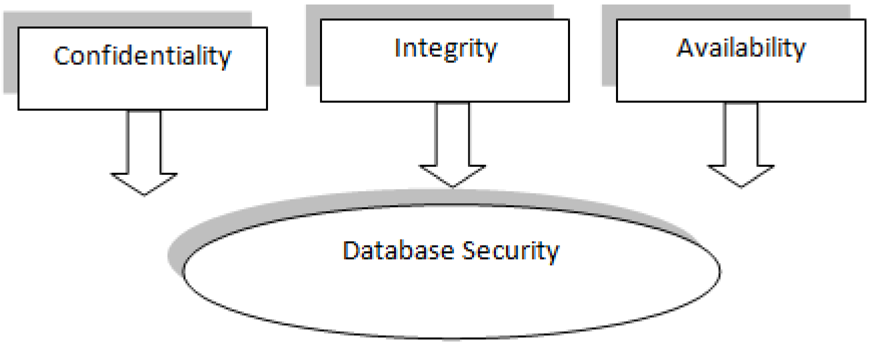

Figure 1:

In today's world security is one of the serious and challenging issue that people are siding all over the world in every slant of their lives. Same as security in electronic world having huge implication. To protect the confidential/sensitive data which is stored in depository is actually the database security [4]. Various security layers in a database exist. These layers are as following: database administrator, system admin, security officer, developers and employee [4] and security can be violated at any of these layers by an attacker.
An attacker can be classified into three classes [4]:

A. *Intruder*

An unauthorized user who inordinately accessing a computer system and tries to fetch beneficial information is called an intruder.

B. *Insider*

A person who is one of the representative of trusted users and misconduct of his/her authority and tries to get information beyond his own allowance is known as an insider.

C. *Administrator*

An administrator is an authorized user who has permission to administer a computer system, but uses his/her administration privileges illegally as per organization's security policy to stalk on DBMS actions and to get important information.

II. DIFFERENT TYPES OF ATTACKS

After breaching through all layer of security, any one of the two following attacks can be carried out by an attacker [5]:

A. 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.

B. 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.

Attacks on database can be further classified into two types [6]:

C. 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.

D. Active Attacks:

In active attack, actual database values are modified. [7]These are more problematic than passive attacks because they can misguide a user. For example a user capturing wrong information in result of a query. [6] 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.

Databases are most favourite objective for attackers because of the data these are containing and their volume [5]. In this paper various threats and challenges in database security are discussed.

III. THREATS TO SECURITY IN DATABASE

A. Excessive Privilege Abuse:

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.

B. 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 [8].

C. 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 [8], which could result in fake accounts, funds transfer, and misunderstanding of certain analytical information [9].

D. 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 [9].

E. 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.

F. Weak Audit Trails

A database audit policy assures automated, on time and appropriate tracking of transactions performed in database [10]. 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 [4].

G. 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. [11].

H. Database Communication Protocol Vulnerabilities

Huge amount of security deficiency is being found in the database communication protocols of all database retailers. Forged activities directing these vulnerabilities can change from illegal data access to data exploitation and denial of service and many more [4].

I. 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 [11].

IV. DATABASE SECURITY CONSIDERATION

To remove the security threats every organization must consists a security policy which should be implemented for sure. A strong security policy must contain well defined security features.

A. Access Control

Access control makes sure that all communications between databases and other system objects are as per the policies and controls defined. No tampering generated by any attacker neither internally nor externally and thus protects the databases from potential errors. 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.

B. Inference Policy :

This is essential to protect the data at some specific level. It comes when the analysis of particular data in the form of facts are required to be prevented at a certain higher security level. Inference policy also helps to determines how to protect the information from being released.

C. User Identification /Authentication:

This is the very basic obligation 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.

D. Accountability and auditing :

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. The data puts on servers for authentication, accounting and access of a user can be analysed with the help of auditing and accountability.

E. 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.

V. CONCLUSION

Data to any organization is a most important property. Protection of crucial data is always a tough task for an organization at any stage. Databases are most favourite n easy target for attackers because of the information it contains and its volume. Database can be accommodated in several ways. Different types of attacks and threats are there today from which a database should be protected. For preventing the sensitive data from attacker which considerations we have to adopt is mentioned in this paper.

REFERENCES

[1] Kadhem, H.; Amagasa, T.;Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on; Publication Year: 2009, Page(s): 163 –170

[2] Luc Bouganim; Yanli GUO; Database Encryption; Encyclo- pedia of Cryptography and Security, S. Jajodia and H. van Tilborg (Ed.) 2009, page(s):) 1-9

[3] Khaleel Ahmad; Jayant Shekhar; Nitesh Kumar; K.P. Yadav; Policy Levels Concerning Database Security;

[4] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,”Database Security and Encryption: A Survey Study”, International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[5] Emil Burtescu, “DATABASE SECURITY - ATTACKS AND CONTROL METHODS”, Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009

[6] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, "Review of Attacks on Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[8] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer, "Database Encryption – An Overview of Contemporary Challenges and Design Considerations", SIGMOD Record, September 2009 (Vol. 38, No. 3).

[9] Khaleel Ahmad; JayantShekhar; Nitesh Kumar; K.P. Yadav; Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368-372

[10] Ravi S. Sandhu, Sushil Jajodia, "DATA AND DATABASE SECURITY AND CONTROLS", Handbook of Information Security Management, Auerbach Publishers, 1993, pages 481-499.

[11] http://www.channelinsider.com/c/a/Security/Database-Vulnerabilities-Top-10-Rules-IT-Shops-Break-772412/.

[12] Shally Rohilla, Pradeep Kumar Mittal; "DATABASE SECURITY:THREATS AND CHALLENGES", IJARCSSE (ISSN: 2277 128X) Volume 3, Issue 5, May 2013,page(s) 810-813.