www.ijarcsse.com

Volume 3, Issue 5, May 2013 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 Challenges

Shelly Rohilla*
Department of Computer Science & Applications,
Kurukshetra University, India

Pradeep Kumar Mittal
Department of Computer Science & Applications,
Kurukshetra University, India

Abstract – Data is the most valuable asset in today's world as it is used in day –to –day life from a single individual to large organizations. To make the retrieval and maintenance of data easy and efficient it is stored in a database. Databases are a favorite target for attackers because of the data these are containing and also because of their volume. There are many ways a database can be compromised. In this paper the challenges and threats in database security are identified.

Keywords – attacks, database security, threats.

I.INTRODUCTION

Data is the most valuable asset in today's world as it is used in day –to –day life from a single individual to large organizations. To make the retrieval and maintenance of data easy and efficient it is stored in a database. Considering the importance of data it is essential to secure it [1]. 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. 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.

An attacker can be categorized into three classes [4]:

A.Intruder

An intruder is a person who is an unauthorized user means illegally accessing a computer system and tries to extract valuable information.

B.Insider

An insider is a person who belongs to the group of trusted users and makes abuse of her privileges and tries to get information beyond his own access rights.

C.Administrator

An administrator is a person who has privileges to administer a computer system, but uses her administration privileges illegally according to organization's security policy to spy on DBMS behavior and to get valuable information.

An attacker, after breaching through all levels of protection, he will try to do one of the two following attacks [3]:

A. Direct attacks

A direct attack means attacking the target directly. These are obvious attacks and are successful only if the database does not implement any protection mechanism. If this attack fails, the attacker moves to the next.

B. Indirect attacks

Indirect attacks are the attacks that are not directly executed on the target but information from or about the target can be received through other intermediate objects. Combinations of queries are used some of them having the purpose to cheat the security mechanisms. These attacks are difficult to track.

The attacker executes the above attacks in different ways.

Attacks on database can also be classified into passive and active attacks [1]:

A. Passive Attack

In passive attack, attacker only observes data present in the database. Passive attack can be done in following three ways:

1) Static leakage: In this type of attack, information about database plaintext values can be obtained by observing the snapshot of database at a particular time.

2) Linkage leakage: Here, information about plain text values can be obtained by linking the database values to position of those values in index.

3) Dynamic leakage: In this, changes performed in database over a period of time can be observed and analyzed and information about plain text values can be obtained.

B. Active Attacks

In active attack, actual database values are modified. [4] These are more problematic than passive attacks because they can mislead a user. For example a user getting wrong information in result of a query. [1] There are some ways of performing such kind of attack which are mentioned below:

1) Spoofing – In this type of attack, cipher text value is replaced by a generated value.
2) Splicing – Here, a cipher text value is replaced by different cipher text value.
3) Replay – replay is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

Databases are a favorite target for attackers because of the data these are containing and also because of their volume [3]. In this paper various threats and challenges in database security are discussed.

II.SECURITY THREATS TO DATABASE

A. Excessive Privilege Abuse

When users (or applications) are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose. For example, a computer operator in an organization requires only the ability 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 misuses their legitimate database privileges for unauthorized purposes. Legitimate privilege abuse can be in the form of misuse by database users, administrators or a system manager doing any unlawful or unethical activity. It is, but not limited to, any misuse of sensitive data or unjustified use of privileges [11].

C. Privilege Elevation

Sometimes there are vulnerabilities in database software and attackers may take advantage of that to convert their access privileges from an ordinary user to those of an administrator [11], which could result in bogus accounts, transfer of funds, and misinterpretation of certain sensitive analytical information [2]. A database rootkit is such a program or a procedure that is hidden inside the database and that provides administrator-level privileges to gain access to the data in the database. These rootkits may even turn off alerts triggered by Intrusion Prevention Systems (IPS). It is possible to install a rootkit only after compromising the underlying operating system [9].

D. Platform Vulnerabilities

Vulnerabilities in operating systems and additional services installed on a database server may lead to unauthorized access, data corruption, or denial of service. For example, the Blaster Worm took advantage of a Windows 2000 vulnerability to create denial of service conditions [11].

E. Inference

Even in secure DBMSs, it is possible for users to draw inferences from the information they obtain from the database. A user can draw inference from a database when the user can guess or conclude more sensitive information from the retrieved information from the database or additionally with some prior knowledge. An inference presents a security breach if more highly classified information can be inferred from less classified information. There are two important cases of the inference problem, which often arise in database systems [5].

1) *Aggregation problem:* occurs when a collection of data items is more sensitive i.e. classified at a higher level than the levels of individual data items. For example in an organization the profit of each branch is not sensitive but total profit of organization is at higher level of classification.
2) *Data association problem:* occurs whenever two values seen together are classified at a higher level than the classification of either value individually. As an example, the list containing the names of all employees and the list containing all employee salaries are unclassified, while a combined list giving employee names with their salaries is classified.

F. SQL Injection

In a SQL injection attack, an attacker typically inserts (or “injects”) unauthorized SQL statements into a vulnerable SQL data channel. Typically targeted data channels include stored procedures and Web application input parameters. These injected statements are then passed to the database where they are executed. For example in a web application the user inserts a query instead of his name. Using SQL injection, attackers may gain unrestricted access to an entire database [11]

G. Unpatched DBMS

In database, as the vulnerabilities are kept changing that are being exploited by attackers, database vendors release patches so that sensitive information in databases remain protected from threats. Once these patches are released they should be patched immediately. If left unpatched, hackers can reverse engineer the patch, or can often find information online on how to exploit the unpatched vulnerabilities, leaving a DBMS even more vulnerable that before the patch was released [7].

H. Unnecessary DBMS Features Enabled

In a DBMS there are many unneeded features which are enabled by default and which should be turned off otherwise they would be the reason for the most effective attacks on a database [10].

I. Misconfigurations

Unnecessary features are left on because of poor configuration at the database level [10]. Database misconfigurations provide weak access points for hackers to bypass authentication methods and gain access to sensitive information. These flaws become the main targets for criminals to execute certain types of attacks. Default settings may not have been properly re-set, unencrypted files may be accessible to non-privileged users, and unpatched flaws may lead to unauthorized access of sensitive data [8].

J. Buffer Overflow

When a program or process tries to store more data in a buffer than it was intended to hold, this situation is called buffer overflow. Since buffers contains only a finite amount of data, the extra data - which has to go somewhere - can overflow into adjacent locations, corrupting or overwriting the valid data held in those locations. For example, a program is waiting for a user to enter his or her name. Rather than entering the name, the hacker would enter an executable command that exceeds the size of buffer. The command is usually something short [6].

K. Weak Audit Trails

A database audit policy ensures automated, timely and proper recording of database transactions [11]. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization’s databases and may cause instability in operations [2]. Weak database audit policy represents a serious organizational risk on many levels.

L. Denial of Service

In this type of attack all users (including legitimate users) are denied access to data in the database. Denial of service (DOS) conditions may be created via many techniques - many of which are related to the other mentioned vulnerabilities. For example, DOS may be achieved by taking advantage of a database platform vulnerability to crash a database server. Other common DOS techniques include data corruption, network flooding, and server resource overload (memory, CPU, etc.) [11].

M. Covert Channel

A covert channel is an indirect means of communication in a computer system which can be used to weaken the system's security policy. A program running at a secret level is prevented from writing directly to unclassified data item. There are, however, other ways of communicating information to unclassified programs. For example, the secret program wants to know the amount of memory available. Even if the unclassified program is prevented from directly observing the amount of free memory, it can do so indirectly by making a request for a large amount of memory itself. Granting or denial of this request will convey some information about free memory to the unclassified program. Such indirect methods of communication are called covert channels [5].

N. Database Communication Protocol Vulnerabilities

Large number of security weaknesses is being identified in the database communication protocols of all database retailers. Fraudulent activities directing these vulnerabilities can vary from illegal data access to data exploitation and denial of service and many more [2].

O. Advanced Persistent Threats

This type threat happens whenever large, well-funded organizations makes highly focused assaults on large stores of critical data. These attacks are relentless, defined, and perpetrated by skilled, motivated, organized, and well-funded groups. Organized criminals and state-sponsored cyber-professionals are targeting databases those where they can harvest data in bulk. They target large repositories of personal and financial information. Once stolen, these data records can be sold on the information black market or used and manipulated by other governments.

P. Insider Mistakes

Some attacks are not intentional, they just happen unknowingly, by mistake. This type of attack can be called as “unintentional authorized user attack” or insider mistake. It can occur in two situations. The first one is when an authorized user inadvertently accesses sensitive data and mistakenly modifies or deletes the information. The latter can occur accidentally when a user makes an unauthorized copy of sensitive information for the purpose of backup or “taking work home.” Although it is not a malicious act, but the organizational security policies are being violated and results in data residing on a storage device which, if compromised, could lead to an unintentional security breach. For example a laptop containing sensitive information can be stolen.

Q. Social Engineering

In this, users unknowingly provide information to an attacker via a web interface like a compromised website or through an email response to what appears to be a legitimate request. An example of this is the RSA breach, which occurred when legitimate users unknowingly provided security keys to attackers as a result of sophisticated phishing techniques [8].

R. Weak Authentication

Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.

1) Brute Force: In this strategy, attacker repeatedly enters username/password combinations until he finds the correct one. The brute force process may involve simple guesswork systematic enumeration of all possible username/password combinations. The attacker can often use automated programs to accelerate the brute force process.

2) Direct Credential Theft: An attacker may steal login credentials from the authorized user.

S. Backup Data Exposure

Backup database storage media is often completely unprotected from an attack as well as a natural calamity like flood, earthquake etc. As a result, several high profile security breaches have involved theft of database backup tapes and hard disks [11].

III.CONCLUSION

Databases are a favorite target for attackers because of their 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. Solutions to most of the threats mentioned above have been found, although some solutions are good while some are only temporary. The various threats to the database are discussed in this paper.

References

[1] 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.

[2] 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.

[3] Emil Burtescu, "*DATABASE SECURITY - ATTACKS AND CONTROL METHODS*", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.

[4] 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).

[5] Ravi S. Sandhu, Sushil Jajodia, "*DATA AND DATABASE SECURITY AND CONTROLS*", Handbook of Information Security Management, Auerbach Publishers, 1993, pages 481-499.
http://searchsecurity.techtarget.com/news/1048483/Buffer-overflow-attacks-How-do-they-work.

[6] https://www.teamshatter.com/topics/general/team-shatter-exclusive/unpatched-databases/.

[7] http://www.appsecinc.com/downloads/Risks to Database Security in 2012.pdf.

[8] http://www.pciguru.com/2012/02/17/2012-database-threats/.

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

[10] http://www.imperva.com/downloads/Top Ten Database Security Threats.pdf.