Database attacks and security: a review

Ms. Mira K. Sadar[*1], Mr. Pritish A.Tijare[*2], Mr. Swapnil N.Sawalkar[*3]

*Department of Computer Science and Engineering, Sipna College of Engineering and Technology, Badnera Road, Amravati, Maharashtra, India.

[1]mirasadar@gmail.com
[2]pritishtijare@rediffmail.com
[3]snsawalkar@rediffmail.com

***Abstract*--Data is most important in today's world. Data plays very important role in various organizations also for the every individual to extract information and helps to take important decisions. This type of data includes the essential information related to individuals or organizations. So to retrieve and maintain the data easily, it is generally stored in database. All the data manipulation and maintenance is done using database management system. Due to large number of data, attacks on database also increasing rapidly. Therefore it is essential to secure database. In this paper we study the different types of attacks and the security techniques of the database.**

Keywords: Database, attacks, SQLIA, security

INTRODUCTION

Data is that the major element on that entire organization depends. This dependency is thus intense that success and failure of organization's goals depends on the standard and amount of information. Thus naturally organizations can't afford to lose very important data concerning the organization and its business.

Nowadays all organizations such as institutes, public, private, governmental, small or large are dependent on computerized information system which includes their daily activity. For such information system there is a database. Major chunk of information are keep within the repository known as database. The information keep in databases are going to be structured and customarily keep within the kind of relative tables as most of the organizations use relative databases. As relative knowledge model is employed, knowledge keep in numerous relative tables are associated with one another. Database management System (DBMS) could be a set of applications that facilitate in managing data within the database.

It helps to arrange data for higher performance and quicker retrieval by maintaining indices. It facilitates conserving logs of transactions that help in regaining data. DBMS performs the activity of concurrency management. DBMS conjointly performs data recovery operations of database.

As data keep in databases is also essential, it's vital to secure it. Database may be attacked in many ways. There's an opportunity of offensive knowledge keep in databases as databases are interfaced with some applications and by hampering the applications; it's potential to attack databases. The situation becomes vital once users of database are leaking the knowledge to outside world. Pc Security perpetually addresses three vital aspects of pc connected system specifically Confidentiality, Integrity and accessibility. Confidentiality ensures that pc connected assets are accessed solely by licensed users. Integrity suggests that computer assets are often changed by documented users within the authorized way. Accessibility ensures that assets are accessible to licensed users at applicable times. Database may be computer asset thus confidentiality, integrity and accessibility ought to be thought-about before applying any security policy on database systems.

There are some security needs for information like physical, logical and element integrity together with auditablity, access management, user authentication and information accessibility [1].Physical information integrity deals with physical issues associated with information like equipment failure. Thus an information ought to be recovered from such reasonably failures. Logical information integrity deals with maintaining and conserving structure and relations during an information. Element integrity preserves the accuracy of knowledge parts. Auditablity ensures chase of changes exhausted the information together with the user's agency did them is feasible. Access management suggests that a user is allowed to access solely licensed information.

There are totally different modes of access on different data things. User authentication deals with substantiating the user's credentials before giving access to any of the data objects within the database. Once documented, information ought to be accessible to users of the system as per their access rights. This feature is named data accessibility [1].

In this paper, we have given a quick description of assorted attacks on databases. Some attacks on databases are inference and SQLIA. In section three of the paper, various techniques which may be used to secure information from the attacks are defined. Some techniques embody access management, encryption and data scrambling.

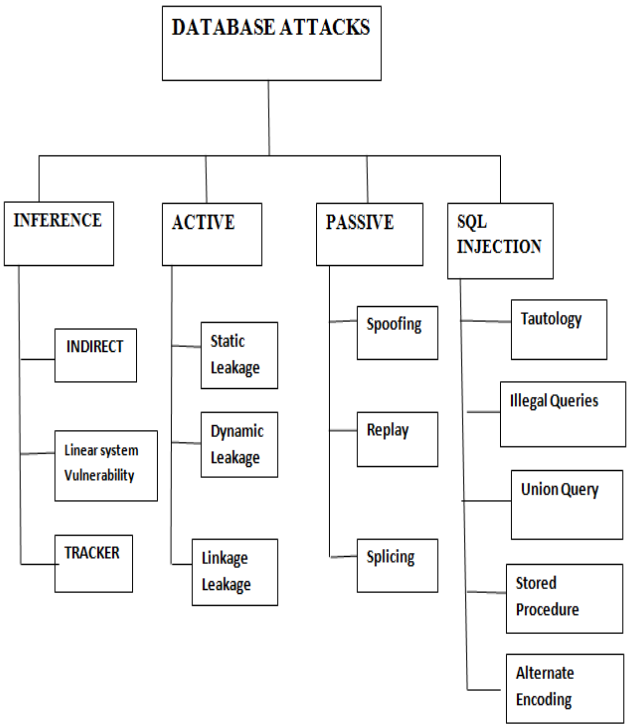
II. DATABASE ATTACKS

As the use of database increases rapidly so the database is going through various attacks. There are some major attacks which are given below:

1. Inference,
2. Active attacks,
3. Passive attacks,

4. SQL injection attack.

These attacks are again classified into various sub attacks which are shown in the following Fig. 1



1 Inference:

Inference may be a major attack on database systems. Inference is way to derives sensitive data from non sensitive data [1]. There's an on the spot attack attainable on database. Inference attack is again classified into three subtypes:

A. Indirect attack: Indirect attacks on information underneath illation embrace use of applied mathematics knowledge to induce the sensitive data. There several ways to own this attack. Attacker might attempt to infer sensitive info from add of some values typically employed in the reports. However this attack is slightly tough. Therefore attacker finds choices having one purpose of intersection that is precisely within the middle.

B Tracker attack: There's another attainable attack underneath inference which is termed tracker attack. In tracker attack, a desired knowledge may be recorded victimization extra queries that turn out tiny results. Attacker adds extra records to be retrieved completely different queries specified two sets of records cancel one another out and solely desired data is left.

C Linear System vulnerability: There's a more general type of a tracker attack referred to as linear system vulnerability. This attack needs very little pure mathematics and logic to search out the data distribution during a database and use it to search out the required components. therefore rather than victimization two opposing query sets, a series of query sets used which is able to cancel one another and eventually desired data is found [1].

2 Passive Attacks:

In active attack, actual information values are modified. This can be a significant quite attack. Active attacks are additional problematic within the sense that they will mislead the user. There are different ways of playing such active attack in which Unauthorized modifications may be created are given below:

A Spoofing: during this kind of attack, cipher text is replaced by a generated value. In this a potential attacker might try and generate a legitimate cipher text, and substitute the present valid value keep on the disk. Assuming that the cryptography keys weren't compromised, this attack poses relatively low risk.

B Splicing: Here, a cipher text value is replaced by completely different cipher text value. In this attack, the encrypted content from a unique location is derived to a replacement location under attack.

C Replay: In this attack exchange a cipher text with associate old version antecedently updated or deleted.

Note that every of the attacks given above under passive attack are extremely correlated to the leakage vulnerabilities of active attacks: static leakage and spoofing, linkage leakage and splicing and dynamic leakage and replay attack.

3 Active attacks: In this attack attacker only observes the data in the database. This attack can be occurred in three ways,

A Static leakage: In this leakage information on the database plaintext values can be gained by observing the snapshot of database at particular time. For example, if the information is encrypted during a manner that equal plaintext values are encrypted to equal cipher text values, statistics concerning the plaintext values, like their frequencies will easily be learned.

B Dynamic leakage: In this leakage, there is Gaining of information concerning the database plaintext values by perceptive and analyzing the changes performed within the database over a portion of time. As an example, if a user monitors the index for an amount of time, and if during this amount of time just one value is inserted the observer will estimate its plaintext value supported its position within the index.

C Linkage leakage: In this leakage gaining of information on the database plaintext values by linking a table value to its position within the index. For example, if the table price and therefore the index price are encrypted in identical manner an

observer will search the table cipher text value within the index, determine its position and estimate its plaintext value.

4 SQL Injection attack:

Nowadays database serve as a backend for many of the web applications. SQL injection attack is one of the serious attacks for such applications. During which malicious SQL statements are supplied into an online kind fields, in web applications, with an intention to hack into the information and place the information contents to the attacker. The attacker influences the queries passed to the database. Many of the web applications use fly on SQL queries without proper user input validation therefore SQL injection attack occurs.

SQL injection attacks categorized into following types:

A Tautology: the main purpose of tautology-based attack is to inject code unconditional statements so they're indefinitely evaluated as true. Using tautologies, the attacker needs to either bypass authentication or insert inject able parameters or extract information from the database. Whenever a conditional statement is injected with code so the result is true, then its analysis and result depends on the method that the query is evaluated within the application. The attacker mainly focuses on the where clause to inject the code. Transforming the conditional into a tautology causes all of the rows within the info table to be return in order that he will login with success while not having a legitimate username and password.

Example:
"SELECT * FROM login WHERE uname = 'mira' and password ='aaa' OR '1 '='1'
The code injected in the conditional (OR '1'='1') transforms the entire WHERE clause into a tautology the query evaluates to true for every row in the table and returns all of them.

B Illegal queries: the main purpose of the Illegal/Logically Incorrect Queries based SQL Attacks is to assemble the information regarding the backend database of the web Application. When a query is wrong or illegitimate, an error message is returned from the database together with helpful debugging data. This error messages facilitate attacker to find vulnerable parameters within the application and consequently database of the application.

Example:
In this example attacker makes a type mismatch error by injecting the subsequent text into the pin input field:

1) Original URL:
http://www.arch.polimi.it/eventi/?id_nav=886

2) SQLInjection:
http:/`/www.arch.polimi.it/eventi/?id_nav=8864'

Error message showed:
SELECT name FROM Employee WHERE id =8864\' from
the message error we can find out name of table and fields:
name; Employee; id. By the gained information attacker can arrange more strict attacks [6].

C Union queries: In this technique, attackers join injected query to the original query by the word UNION and then can receive data concerning other tables from the application. The output of this attack is that the database gives a dataset that is the union of the results of the initial query with the results of the injected query.
Example:
SELECT Name, Address FROM Users WHERE Id=$id
By injecting the following-
Id value: $id=1 UNION ALL SELECT creditCardNumber,1 FROM CreditCarTable.
We will have the following query: -
SELECT Name, Address FROM Users WHERE Id=1 UNION ALL SELECT creditCardNumber, 1 FROM CreditCarTable
which will join the result of the original query with all the credit card users.[6]

D Stored procedures: This type of attack tries to execute stored procedures present in the database with malicious inputs. As stored procedure may well be coded by programmer, so, this part is as inject able as web application forms. Depend upon specific stored procedure on the database there are alternative ways to attack.
For example:-
SELECT accounts FROM users WHERE login= '1111' AND pass='1234 '; SHUTDOWN;--;
this type of attack works as piggyback attack. The first original query is executed and consequently the second query which is illegitimate is executed and causes database shut down. So, it is considerable that stored procedures are as vulnerable as web application code.

E Alternate encoding: The attacker uses Alternate Encodings like, ASCII, Unicode, EBCDIC and positional representation system to inject code in order that it will bypass the validations on the input, if any.

Example –
Original Query- „Select * from login where username = „a123‟ and pwd="xxx""
Injected Query- „Select * from login where username = „ "; exec(char(0x73687574646f776e)) --" and pwd="not required""
The value passed to the char() perform is that the hexadecimal coding for SHUTDOWN. Therefore because the on top of injection uses hexadecimal coding rather than actual characters, it'll bypass the input validations and can cause the SHUTDOWN command to be execute.

III DATABASE SECURITY:

As the organizations, institutes, small, large companies etc raised their adoption of database systems as the unique data management technology for daily operations and decision making, the security of data managed by these systems becomes critical. Damage and misuse of data affect not only a single user or application, but may have great consequences

on the entire organization. The recent rapid production of Web based applications and information systems have further raised the risk exposure of databases and, thus, data protection is today more crucial than ever. It is also important to value that data needs to be protected not only from outer threats, but also from insider threats.

Following are some techniques used for database security:

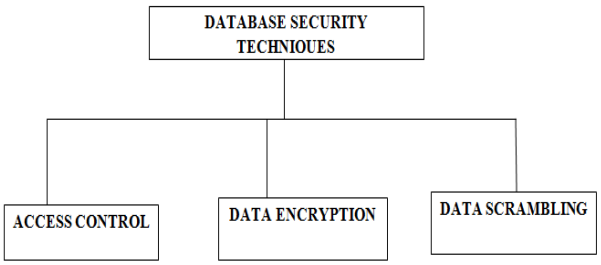


Fig. 2 Database security techniques

1 Access Control: Access control is the greatest security technique for database. It ensures the data confidentiality. Once somebody tries to access data object, Access control Mechanism checks the rights of the user against set of authorizations.[4]
Access control is divided into following types:

A Discretionary access control: This governs the access of users to the knowledge on the premise of the user's identity and authorizations. These authorizations also referred to as rules. These rules specify the access modes, for every user and every object within the system. Discretionary Access control (DAC) are often referred as a way of restricting access to things supported the identity of subjects or teams to that they belong.DAC places the choice of who will access information at the discretion of data creator i.e. owner of database administrator. Security policy implementation is predicated on granting and revoking privileges. Access is granted or denied based on the identification of the user. The Authorization Administration Policy supervises this function in DAC. Common Administration Policies used in DAC are Centralized Administration and Ownership Administration. In centralized administration just some privileged subjects could grant and revoke authorizations whereas in possession administration grant and revoke operations on data objects are entered by the creator of the object.

B Mandatory access control (MAC): This constrains the power of a user to access or usually perform some kind of operation on an object. Water proof policy needs all users to follow the principles of access established by the database Administrator (DBA). This policy desires objects (e.g. Database) to be classified and subjects (e.g. Users, Process) to be cleared. It is enforced by scrutiny attributes of an issue and an object to regulate access to the thing. It restricts access to things supported the sensitivity of the data. It conjointly provides surroundings that restrict users to sharing data solely among identical project, department or organization.
C Role Based Access Control (RBAC): This represents very important new innovation in access control mechanism. RBAC has been inspired by the need to simplify authorization administration and to directly represent access control of organizations. Role-based policies regulate user's access to the information on the basis of the activities the users execute in the system i.e. RBAC models are based on the notion of role. A Role shows a specific function within an organization and can be seen as a set of actions related with this function. Under an RBAC model, all authorizations needed to act a certain activity are granted to the role related with that activity, rather than being granted directly to users. [2]
2 Data encryption:
Data encryption is one of the basic techniques used for securing any type of data. Encryption is the process in which plaintext is converted into cipher text. Plaintext is nothing but the user's original data and cipher text is the scrambled data which is obtained after applying the encryption to plaintext. Fig. 3 shows the basic structure of encryption technique.

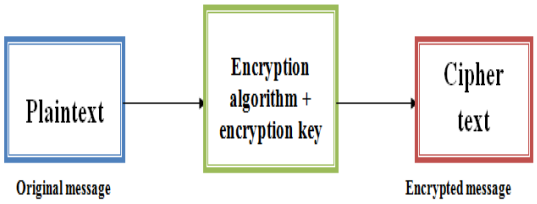


Fig. 3 Basic encryption structure

This technique is also applied to the database. Figure 3 shows the basic structure of encryption. Message encrypted using encryption keys and encryption algorithms. Encrypted message is then stored in the database and decrypted when it is need to be used for further process. There are two types of encryption commonly used. Symmetric Encryption is the type of encryption where only one private key is used for both encryption and decryption. Asymmetric encryption is the type where a two of secret keys are used. One keys is used for encryption and the other used for performing database decryption, a decision about whether to perform the encryption inside database or outside the database must be taken. Some of the issues involved in this technique are How to protect keys from attacker? How to give rights of manipulating information using keys? And How to provide limited access for keys?
The algorithms which are commonly used for encryption are RSA, AES, DES, 3DES, RC2 etc.

There are various configurations present for encryption of database some of that are given below:

A File System Encryption: In this encryption entire physical disk where the database resides is encrypted .In this database

is encrypted using single key so the discretionary access control cannot be supported.

B DBMS Level Encryption: There are many methods for this type of encryption. One method is based on Chinese Remainder theorem in which each row is encrypted using different sub-keys for different cells. This method enables encryption at the level of rows and decryption at the level of cells. Another method proposes encryption for a database depends on Newton's interpolating polynomials.

There is a SPDE method which encrypts each cell in the database with its cell coordinates like table name, column name and row id etc. So in this method static leakage attacks and splicing attacks are prevented.

C Application level Encryption: In a Web Data Service Provider Middleware (WDSP) application is defined which translates the user queries into a new set of queries which execute of the encrypted DBMS. The model was implemented as the Data Protector System which serves as an http level rule-based middleman who regulates access to secure data stored on web service provider. The solution is attractive to public data storage; this method is based on data protector.

D Client-side encryption: The recent rapid increase in Internet usage, along with advances in software and networking, has resulted in organizations can easily share information for a different type of purposes. This defines to a new pattern termed "Database as a Service" (DAS) in which the whole process of database management is outsourced by enterprises to reduce value and to concentrate on the basic business.

One essential problem with this architecture is data privacy. That is, sensitive information has to be securely stored and protected against untrustworthy servers. Encryption is one efficient solution to this problem. [2]

3 Data scrambling: Data Scrambling could be a method of creating sensitive information in non-production databases safe for wider visibility. Data scrambling is additionally referred to as data sanitization, data masking and data obfuscation.

Data scrambling is mostly used once users have correct access to data within the database however still it is needed to secure sensitive information from them. Samples of such users are often third party developers or testers acting on data in database. That values of the database that are unit sensitive are modified however still the values are unit realistic in nature.

The main secure ways of scrambling are extract data through scrambling functions on either live copy or ideally on the coverage copy of production data, build a collection of views which may be accustomed mask the database and make a secure atmosphere, take copy of production data, update data and so complete copy to development.

Traceability is one amongst the advantages of scrambling that is very important just in case of information loss. Scrambling is a lot of through and a lot of helpful to testing groups. Scrambling for brand new releases of package is mechanically upgraded as a region of traditional life cycle.

While scrambling database data, it's necessary to grasp foreign key constraints, relationships between totally different columns of database tables, correct documentation of ways used for scrambling. Totally different scrambling ways are straightforward freelance functions to place random text, dates and numbers, multi table column values and offset values. Some sources of scrambling ways are database functions that area unit inbuilt functions in software system, some tools for scrambling like data Maker, customized code for the system into consideration and a few database sources like books, journals and web. Using Seed Tables is additionally a good technique for scrambling data. These tables are often static or dynamic in nature.

There are some problems in data scrambling. The scramble data should assemble original data. Contents in one column in row are associated with contents in alternative column in same row. Scrambled values ought to conjointly maintain same relationships. Rows within the table area unit DE normalized and contain database that's identical among several rows. Scrambled values ought to conjointly maintain identical relationships. Typically data that is covert are often used as is part of key to columns in several alternative tables. Thus knowledge covert in one table should be synchronal with data changes in range of alternative tables. It's combination of Row internal, table internal and table-table knowledge synchronization. The keys ought to be disorganized in intelligent ways that in order that constraints shouldn't be desecrated. Matter knowledge, memos and letters etc. are troublesome to scramble. Thus for such cases the intelligent ways of scrambling ought to be adopted.

For scrambling data a care should be taken that a scrambled value should not overflow previously defined limit of data. Data across all row columns should remain consistent. Sometimes separate data is not attributable but collection of data may be sensitive. During scrambling Decision about what data should be scrambled and what not to be scrambled is important.

CONCLUSION

Today the database acts as very important backbone for various organizations. So the attacks on database are increases. There is lot of scopes to improve techniques of security. In this paper we review the different types of attacks on database such as inference, active attacks, passive attacks and SQL injection are discussed, also some security techniques that are being employed presently to augment and enhance the security of the database systems were explained.

REFERENCE

1] Pfleeger ,ISecurity in Computingl, fourth edition,2004, Pearson education

2] "Database Encryption – An Overview of Contemporary Challengesand Design Considerations", SIGMOD Record, September 2009 (Vol. 38, No. 3)

[3] Mr. Saurabh Kulkarni1, Dr. Siddhaling Urolagin2, "Review of attack on database and security techniques" ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[4]Jasdeep Singh Bhalla,"A Database Encryption Technique to Enhance Security Using Hill Cipher Algorithm",IJEAT, ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[5] Akshay Patil* and Prof. B. B. Meshram, "Database Access Control Policies", IJERA, Vol. 2, Issue 3, May-Jun 2012, pp.3150-3154

[6] Neha Mishra1, Sunita Gond2, "Defenses To Protect Against SQL Injection Attacks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013
[7] 1Dr. T. N. Sharma, 2Amitesh Kumar, 3Sumitra Singar, 4Vishakha Singhal, "A Propose Model for Prevention of Attack SQL Injection",IJCST Vol. 4, Iss ue Spl - 2, April - June 2013

