Database Security: Attacks and Techniques

Preeti Sharma

Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119

Email: preetisharma4795@gmail.com

Monika

Department of Computer Science & Applications, Kurukshetra University, Kurukshetra-136119

Email:

ABSTRACT

In today's world, the data become an essential asset as it is used in daily life from a single person to every big organization. To make the use of data efficient and maintained it is stored in database. Hence the database security is an important factor to provide integrity, confidentiality and availability of data. This paper generally provide a review of need of database security, attacks possible on databases and their prevention techniques.

Keywords- Access Control, Active Attack, Attacker, Database, SQLIA.

1. INTRODUCTION

The data plays an crucial role in today's world for the success or failure of an organization because mostly of the organizations make the use of database for storage of major or important data of the organization and the data is not mandatory to be an user's details but it also contains all credential or sensitive information of an organization. Many of the organizations spent lot of money for securing their databases and this importance of data will make the database security important in every sector either it is private sector or government sector. Hence the data must be protected.

Basically there are five layers of security – database admin, system admin, security officer, developer and employee. Thus, security can be affected at any of the level by an attacker. In database security attackers are divided into three segments that are -

1.1 Administrator

An admin is an authorized person who has permission to control the system but misuses his/her privileges against the security policies to get the important information.

1.2 Insider

An insider is also a member of trusted committee in an organization but did misuse of his/her authority and want to get some sensitive or any other important information.

1.3 Intruder

An intruder is not a part of an organization. Actually he/she is unauthorized people who access the personal data of an organization and want to get the sensitive information.

The security of data basically requires three things-Confidentiality, Integrity and Availability. Where Confidentiality means the data must be used by an authorized person, Integrity means the data must be controlled by an authorized person in an authorized manner and Availability means the data must be available to an authorized user at appropriate time. These three are shown in Fig.1 below:

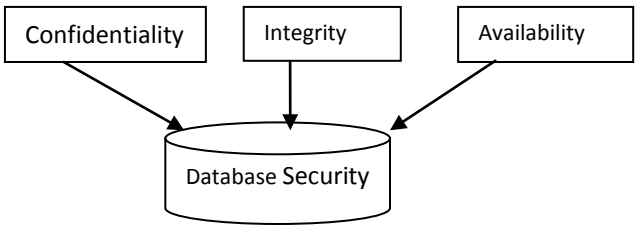

Fig.1 Three main factors of database security

2. ATTACKS ON DATABASE

The attacks performed on database are basically classified into two segments:

2.1 Passive Attacks

Passive attacks focus on the observation. Here the attacker observes the data present in the database. The passive attack is very dangerous attack but less problematic than active attacks. Generally, passive attacks are performed without any data modification. In passive attacks no data in the database is to be modified but the attacker just observes the communication between two users over the network. The passive attacks can be performed in three forms:

2.1.1 Static Leakage

In this type of passive attack, the snapshot of database is observed in the sense to obtain the plain text values at a particular specified time. Static leakage only deals with the observation of the data in database only at a specified time period but after a time the attacker stop the observation on data Basically, it is not much harmful because data remains same and appropriate data is received by the right person but the attack performs because the attacker just observe the data in database. It is called static leakage because it is performed only for a specified time period.

2.1.2 Linkage Leakage

In this type of passive attack, the linking between the database value and the position of that specified value in index is established to obtain the plain text value. In linkage leakage, some steps are taken to actually perform the linkage attack. First step in linkage leakage is to check the index of the database and search for the particular data on which the attack is to be performed. And in second step, when the required data value is found in an index of the database, the data get linked with the database value. Linkage leakage creates problems but it is not as dangerous as compared to other attacks

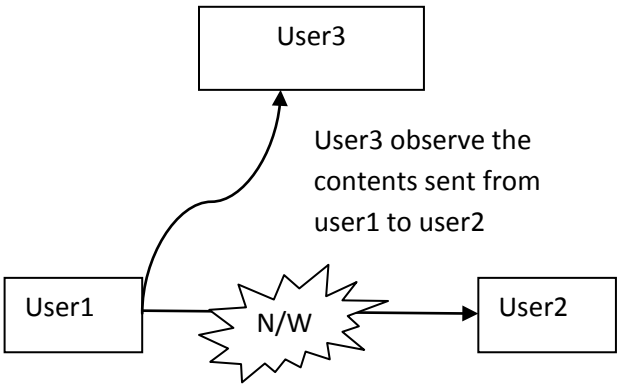

Fig.2 Passive attack

2.1.3 Dynamic Leakage

In this type of passive attack, the plain text value can be generated by observing the continuous changes performed in database for a particular time. Then after observing the changes the data is analyzed that help the attacker to get the related data about the plain text value.

The main steps in dynamic leakage are –In first step, the attacker observe the data transmitted between users for a time and in second step, the observed data is analyzed that results in the related information of the plain text value.

2.2 Active Attacks

The active attack is much more problematic as compared to the passive attack because passive attack is based on the observations and no modification in data can be done in passive attack. But in active attack, the modification of data is done For example; the user captures the wrong information as result of query. The active attack can be performed by different ways as:

2.2.1 Spoofing

In this active attack, a value is generated and then the cipher text is replaced by that value. This value is generated by using some algorithms and techniques.

2.2.2 Splicing

In this active attack, two cipher text values are there and one cipher text value is then replaced by another cipher text value.

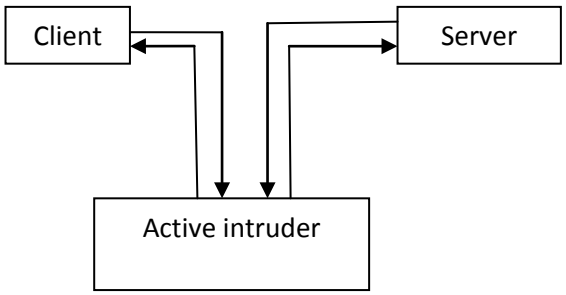

Fig. 2.2 Active attack

2.2.3 Replay

In this active attack, the cipher text value is replaced by old version that is previously updated or may be deleted. That's why this attack is called replay because deleted old version value is under consideration.

2.3 SQL Injection Attack

SQL injection attack is the most serious attack in the database security. In today's world almost all applications use the database as backend and the most critical attack placed on the web applications is SQL injection attack that is abbreviated as SQLIA or SIA. Basically SQLIA can be termed as the dangerous attack in database security because SQL attack is performed on server and then server run the malicious queries that results in the manipulation of the database. SQL injection is just a technique in which malicious users can add the SQL commands into the SQL statements, through web page input.

Here, an executor normally adds the unauthorized database statements into an unsecure SQL data channel. The SQL injection attack is basically performed to allow the unauthorized access to the database.

SQL injection attack is divided into some attacks that are given as:

2.3.1 Tautology Based Attacks

Tautology attack is generally occurred in database because these are very simple to perform. Here , attacker uses one or more than one conditional statements by injecting SQL tokens so that it is always evaluated true i.e. 1n these attacks, attacker normally traverse the authentication pages and access these pages that helps for execution purpose. For example,

"SELECT name FROM bank WHERE name=' ' or1=1--'AND pin =' '

In this example the code is injected at WHERE clause and the data is easily retrieved because the where clause always return true. The database treats everything after WHERE token as conditional statement but inclusion of "OR 1=1" clause turn it into tautology (The character "--"begins the comment that everything after this is ignored.)

2.3.2 Union Queries Based Attack

In tautology attack the data retrieval is not possible. But in the union query based attack, attackers make the use of unsecure parameter to make injected data and then join this injected query to the original query using UNION. Hence this can retrieve the data from the database.

For example, "SELECT name FROM bank WHERE name=''UNION SELECT name from employee WHERE employee id='123' -- AND pin=

Suppose that there is no name equal to "" (empty string), the original query returns null string, the injected query returns name of employee with employee id '123'. Thus, the final result is union of two queries and finally returned by application.

2.3.3 Piggybacked Queries

It is the one of the most harmful attack because in this attack no effect is visible on original query but similar to union query attack an injected query is added to the original query.

For example, "SELECT name FROM bank WHERE name='Preeti' AND pswrd ='abcde' AND pin='132001'; drop table bank

Here, the database treats the query as two queries separated by delimiter (;) and execute the both where first one is original and second one is injected query. Hence this injected query drops the bank table into the database.

3. DATABASE SECURITY TECHNIQUES

There are many database security techniques that help us to secure the data objects in the database. These techniques are discussed below:

3.1 Access Control

Every organization has its own security officer who provides the different access to the different users according to the security policies of an organization. The access control techniques manage the confidentiality of the data. If any user wants to access any of the data object from the database then this access control mechanism will check the rights given to that particular user. A very strong authentication method is required to authenticate the valid users of the database system. There are two models which give us brief idea that how the accesses control mechanisms are implemented on the database system that are given as:

3.1.1 Discretionary Access Control Model

In this model, two factors are considered while giving access to user that are -identity of user and authentication policies of organization. The access is given to the users according to some discretionary rules. In this approach, the concept of authentication administration is used that is just a function of grant and revoke authorization. Here the authorization can be easily removed from or included into the access control mechanism.

3.1.2 Mandatory Access Control Model

This access model is based on the categorization of the data object and users. Categorization focuses on a partially ordered set of class that is access class and this access class has multiple groups of categories and security level. Access control in the access model are based on two factors

3.1.2.1 No Write- Down

The user can only writes the data objects whose access class dominates by access class of the user.

3.1.2.2 No Read-Up

The user can only read those data objects whose access class dominates by access class of the user.

3.2 **SQLIA Fighting Techniques**

SQLIA attack is the most serious attack in the database system so there are many techniques that are help to prevent from SQLIA like pre-generated approach and post-generated approach. Post – generated approach is used in analysis phase and pre-generated approach is used in testing phase of the web application. Some approaches are:

3.2.1 Positive Tainting and Syntax aware evaluation

In positive tainting we give the valid input to the system for detection of SQLIA that help us to differentiate between the valid and invalid input strings and then syntax aware evaluation is done on propagated string to differentiate the non trusted string from the trusted string.

3.2.2 Context Sensitive String Evaluation

Syntax analysis is done to categorize the string and numeric constants and then all unsecure characters are removed from alpha numeric identifiers.

Here, data given by user is taken as non- trusted and the data given by the application is treated as trusted.

Basic steps performed in this technique are:

Step1) Untrusted data about data is used for analysis of syntax.

Step2) Syntax analysis separates the string and numeric constants.

Step3) Unsecure data is removed from alpha numeric identifiers.

3.3 Data Encryption

This is the very basic and widely used method for database security. In this technique , any kind of data or information can be encrypted in the form that an unauthorized person cannot able to recognize the actual content .Thus it provide the security among the transmission of messages from one person to other in an encrypted format.

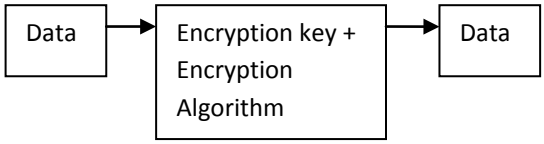

Fig.3.3 Encryption Process

The data encryption is done using encryption keys and encryption algorithm. Hence it is very important to secure these encryption keys from attacks with the help of different encryption techniques. The data encryption needs a decision that whether the encryption is done inside or outside the database.

3.4 Data Scrambling

The data scrambling is also known as data sanitization, data masking and data obfuscation. This technique is generally used in the cases where the user have right to access the data objects of database but still want to secure the sensitive data from the attackers. Such users like testing team workers, developers. Hence, values of sensitive data are changed but still the values are real in nature.

4. CONCLUSION

The database security is called backbone for every organization as databases are primary storage for data. So many dangerous attacks are done on databases day by day. The general attacks performed on databases are discussed in this paper. Review of some techniques is also discussed such as access control, SQLIA fighting techniques, data encryption and data scrambling. But still we have many of the attacks that have no solution. This paper helps the researchers regarding knowledge of attacks and prevention techniques in databases.

REFERENCES:

Almutairi, Abdulrahman Hamed, and Abdulrahman Helal Aluwaili. "Security in Database Security." *Global Journal Of Computer Science & Technology Network,Web Security.* 2012.pages 9-13.

Basharat, Iqra, Farooque Azam, and Miuzaffar Wahab. "DATABASE SECURITY AND ENCRYPTION : A SURVEY STUDY." *International Journal Of Computer Applications.* 2012.

Begum, Miss. Rehana,, Mr. R.Naveen Kumar, and Mr. Vorem Kishore. "Data Confidentiality Scalability and Accountability (DCSA)." *International Journal of Advanced Research in.* 2012. pages 200-202.

Burtescu, Emil. "Database Security-Attacks & Control Methods." *Journal Of Applied Quantitative Methods.* 2009 pages . 1-4.

Deepika, and Nitasha Soni. "Database Security: Threats and Security Techniques." *International Journal of Advanced Research in Computer Science and Software Engineering.* 2015 pages. 621-625.

Gandhi, Mihir, and Jwalant Baria. "SQL INJECTION Attacks in Web Application." *International Journal of Soft Computing and Engineering (IJSCE).* 2013.page 189.

Halfond, WilliamG.J., and Alessandro Orso. "DetectionandPreventiono fSQLInjectionAttacks ." 2012.pages 86-90.

Harish C. Sharma, Sanjay Sharma , Sandeep Chopra ,Pradeep Semwal. "The Protection Mechanism against DOS and SQL Injection Attack in SIP Based Infrastructure." *International Journal of Advanced Research in Computer Science & Software Engineering.* 2013. pages 252-254.

Kulkarni, Mr. Saurabh, and Dr. Siddhaling Urolagin. "Review of Attacks on Databases and Database Security ." International *Journal of Emerging Technology and Advanced Engineering.* 2012.pages 253-262.

Kumar, Manish, and L.Indu. "Detection and Prevention of SQL Injection attack." *International*

Journal of Computer Science and Information Technologies,. 2014.page 374.

Malik, Mubina, and Trisha Patel. "DATABASE SECURITY - ATTACKS AND." 2014.pages 1-8.

Manmadhan, Sruthy, and Manesh T. "A METHOD OF DETECTING SQL INJECTION ." *International Journal of Distributed and Parallel Systems (IJDPS).* 2012 pages. 1-5.

Murrey, Meg Coffin. "Database Security: What Students Need to Know ." *Journal of Information Technology Education.* 2010.pages 61-77.

Pfeeger. *Security In Computing.* 2004.

R. Gaikwad, Tejashri, and A. B. Raut. "A Review on Database Security." *International Journal of Science and Research (IJSR).* 2014. pages 372-374.

Rafiq, Mohammed. "Database Security Threats & Its Techniques." *IInternational Journal Of Advanced Research In Computer Science & Software Engineering.* 2014. pages 183-185.

Rohilla, Shelly, and Pardeep Kumar Mittal. "Database Security by Preventing SQL Injection Attacks in Stored Procedure." *International Journal of Advanced Research in Computer Science and Software Engineering.* 2013 pages. 915-917.

—. "Database Security: Threats and Challenges." *International Journal of Advanced Research in Computer Science and Software Engineering.* 2013.pages 810-813.

Sandhu, Ravi S., and Sushil Jaljodia. *DATA & DATABASE SECURITY & CONTROLS.* AUERBACH PUBLISHER, 1993.

Singh Chouhan, Arun, and Shalini Aggarwal. "Design & Analysis Of new encryption-decryption algorithm for enhanced cloud Security." *International Journal of Advance Research in Computer Science and Management Studies.* 2015. page362.

Singh, Neha, and Ravindra Kumar Purwar. "SQL INJECTIONS – A HAZARD TO WEB APPLICATIONS." *International Journal of Advanced Research in.* 2012.pages 42-45.

Tajpour, Atefeh, Suhaimi Ibrahim, and Mohammad Sharifi. "Web Application Security by SQL Injection DetectionTools." *IJCSI International Journal of Computer Science Issues.* 2012 page. 332.

U. Randive, Prerna, Mahadev B. Khatke, and Malu B. Reddi. "An Approach for Prevention of SQL Injection Attacks on ." *International Journal of Innovative Research in Advanced Engineering (IJIRAE).* 2014. pages 38-41.