Security Issues and Their Techniques in DBMS - A Novel Survey

Mohd Muntjir
College of Computers and Information Technology
Taif University, KSA

Sultan Aljahdali
College of Computers and Information Technology
Taif University, KSA

Mohd Asadullah
College of Computers and Information Technology
Taif University, KSA

Junedul Haq
College of Computers and Information Technology
Taif University, KSA

ABSTRACT
Nowadays a Database security has become an important issue in technical world. The main objective of database security is to forbid unnecessary information exposure and modification data while ensuring the availability of the needed services. A numbers of security methods have been created for protecting the databases. Many security models have been developed based on different security aspects of database. All of these security methods are useful only when the database management system is designed and developing for protecting the database. Recently the growth of web application with database at its backend Secure Database Management System is more essential than only a Secure Database. Therefore this paper highlight on the Threats, Security Methods and Vulnerabilities in Database Management System with the help of survey performed on the field of secure databases.

Keywords
Vulnerability, threats, security methods, DBMS

1. INTRODUCTION
These days including the invention of internet technology securing database is a needed aspect in today's world. Individually we use database every day unknowingly when we browse on internet. The information we get on the web page is the consequences of query accomplished by the webpage to the database it is connected. Hence indirectly via the webpage we are connected to different databases. The web pages are open for any anonymous person in the world or we can say the databases are indirectly opened for everyone. As we know data in the database is the most valuable asset which can be the source of information. All the information cannot be revealed for everyone. Hence many security tools have been devised to protect the database. As the database is accessible via web pages security should be implemented in database management system (DBMS).Looking towards the implementation this paper focus on Vulnerabilities in Database Management System (VDBMS), Threats in Database Management System (TDBMS) and Security Methods in Database Management System (SMDBMS).

Rest of the paper is organized as follows: section II provides overview of recent trends in database protection, section III, IV and V are devoted to VDBMS, TDBMS and SMDBMS.

Section VI deals with the summary of above section in a tabular format and section VII deals with the conclusion.

2. PROTECTED DATABASE
There are many ways of securing the database. These ways are based on different aspects of securing the database. Different aspects with traditional approaches from different researchers view are summarized below:

2.1 Confidentiality, Integrity and Availability (CIA) in Database Management System
As mentioned in [1] a complete solution to data security must fulfilled the following three requirements Confidentiality, Integrity, Availability (CIA): these entire factors can gained in database using following ways:

2.1.1 Confidentiality
Means to the protection of data against unauthorized disclosure can be achieved using access control mechanism. It is already further enhanced by the use of encryption techniques is applied to data when being stored on secondary storage or transmitted on a Network.

2.1.2 Integrity
Means to the prevention of unauthorized and improper data modification and can be achieved in combination of access control mechanism by semantic integrity constraints.

2.1.3 Availability
Means to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system inaccessible. The data that are available on the Web can be powered by the use of techniques protecting against denial-of-service attacks and such as the ones based on machine learning techniques.

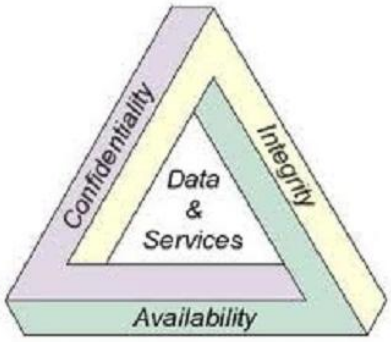

Fig. 1 CIA Triad

2.2 Different Aspects
Latest approaches of protecting database are illustrated in [2]. All of these approaches are related to CIA. In these approaches the author proposes that it can be implemented with the help of below listed appropriate techniques:

2.2.1 Authentication of Users
Within this point the author has mentioned about public key encryption (PKI) for the databases that require higher levels of safety one-time passwords X.509 digital certificate smart cards can be used. PKI is very useful when contacting over irrelevant networks like the Internet and both on the internal servers.

2.2.2 Access control to objects and authentication of authorized applications
In this point means the access control should be defined at the design state. Here main emphasis is given on the roles and based on this access is given to the user.

2.2.3 Administration policies and procedure
Its mean Security and safety policies with plans are required for varying requirements of data security.

2.2.4 Secure initial configuration
This point indicates the Policies and procedures also define auditing requirements for securing initial configuration and managing change regulation.

2.2.5 Auditing
This point refers for auditing the author emphasizes on maintaining logs of the changes to the database management system.

2.2.6 Backup and recovery strategies
This point refers to the backup and strategies, As the backup and recovery there should be three kinds of backup's cold, hot and logical. All these aspects are traditional and there are vulnerabilities in these security methods which may cause threats to the database system. Henceforth this paper gives the detailed information about the vulnerabilities, threats and different security methods to avoid them.

3. ABOUT THE VULNERABILITIES IN DATABASE MANAGEMENT SYSTEM (VDBMS)
Based on our survey conducted the vulnerabilities in database are defined as: poor architecture, misconfigurations, and vendor bugs incorrect usage [2].

3.1 Vendor bugs refer to buffer overflows and other programming errors that result in users executing the commands they are allowed to be execute. Furthermore Downloading and applying patches usually fix vendor bugs and viruses.

3.2 Poor architecture refers the result of inadequate factoring security into the design of how an application works there. These vulnerabilities are typically the hardest to fix because they require a major rework by the vendor. We can give an example of poor architecture; it would be when a vendor utilizes a weak form of inscription.

3.3 Misconfigurations are caused by not accurately locking down databases. Mostly the configuration options of databases can be set in a way that compromises security and safety for that database. Some of these parameters are concluded insecurely by default. But mostly it is not a problem unless you unsuspectingly change the configuration and setting. An example of this in Oracle is the REMOTE_OS_AUTHENT parameter. When you set REMOTE_OS_AUTHENT to true you are allowing unauthenticated users to connect to your database, so that he can do his task correctly.

3.4 Incorrect usage means to building applications utilizing developer tools in ways that can be used to break into a database. SQL injection is an example of incorrect usage for developer.

The authors Marco Vieira and Henrique Madeira [3] have defined that the vulnerabilities in DBMS are an internal factor related to the set of security mechanisms available or not available in the database, the correct configuration of those mechanisms (it is a responsibility of the DBA), and the hidden flaws on the system configuration.

He has described that security in database can be violated due to points as given below:

3.5 Irresponsible DBA: Refers to deactivation of the necessary security mechanisms such that user privileges, authentication, auditing, data encryption which allows intruders to find a way to getting access the data into database.

3.6 Incorrect configuration: Permits unauthorized users or hackers to access the data in our system.

3.7 Hidden flaws in the database: May allow hackers to connect to the database server by exploring those faults.

3.8 Unauthorized users: Means these users "still" the credentials of authorized users in order to access the database server for searching the data.

3.9 Misused Privileges: Refers to authorized users take advantage of their privileges to maliciously access or destroy our data in a database.

Vulnerabilities are also defined by Hassan A. Afyouni [4] in the following manners:

3.10 Configuration and Installation: Using a default installation and configuration that is known by publicly. For example failure to change default password or default privileges or permissions.

3.11 User Mistakes: Sometimes Carelessness in implementing procedures failures to follow directly, or accidental errors with some faults. For example users lack bad authentication process, technical information or implementation, untested disaster recovery plan in a database.

3.12 Software: Refers to vulnerabilities found in commercial software for all types of programs such that all applications, operating systems, database management systems and network systems with other different programs.

3.13 Design and Implementation: Inaccurate software analysis and design as well as coding problems and faults may lead to vulnerabilities in a database.

4. ABOUT THE THREATS IN DATABASE MANAGEMENT SYSTEM (TDBMS)
Threat in database is defined by Aziah Asmawi in [5] as a set of policies, measures and mechanisms to provide safety, availability and integrity of data and to combat possible attacks on the system from outsiders as well as insiders, both accidental and malicious. Aziah Asmawi has mentioned about SQL injection which can be executed by two ways by unauthorized user accessing the database via webpage connected network:

4.1 Access through login page: This is the easiest technique in which it bypasses the login forms where users are authenticated by using password. This type of technique can be done by the attackers through: *'or' condition*, *'having' clause*, *multiple queries* and *extended stored procedure with package*.

4.2 Access through URL: The attackers use this technique through: manipulating the query string in URL and using the SELECT' and UNION statements.

Further Ravi Sandhu [1] has described in his paper that threat to the database can be internal or external. By this technique he has characterized the security breach as incorrect data modification, unauthorized data observation and data unavailability.

As mentioned in [4] types of threats are following:

4.3 People: In this point the different people involved in database management system can be a government authority , an employee or a person-in charge, consultants, contractors, visitors, hackers, organized criminals, spies, terrorists and social engineers may deliberately or unintentionally exact damage on any of the database environment factor.

4.4 Malicious Code : Refers to Software code , in which most cases is intentionally written to damage or violate one or more of the database environment components are boot sector worms, viruses, spoofing code Trojan horses, denial-of-service flood, bots, root kits, bots,

E-mail spamming, macro code.

4.5 Natural disaster: Calamities caused by nature can destroy any or the entire database environment components.

Technological disasters: Refers to Some sort of malfunction in hardware or equipment, technological disorders like media failure, hardware failure, power failure, or network failure can inflict damage to database management systems, data files or data or whole database.

5. SECURITY METHODS IN DATABASE MANAGEMENT SYSTEM (SMDBMS)

Here we will discuss about some security methods in DBMS. In early days security methods in database management system focus only on role base access control or maintaining the confidentiality or authenticity of the database. But in the current scenario the unauthorized user working on a web page which is connected via internet connection has access to the database, since all the queries sent by the user is converted to SQL query in that database. The user may send malicious query and confirm or modify the transactions of the database without affecting the performance of the database. This type of attack is called SQL injection. But in the current scenario the security method of database should focus on role base access control and maintain CIA and avoid attacks due to network. This section emphasizes the same, based on various papers and books available on similar topic or same issue.

5.1 A SECURING DATABASE BASED ON ACCESS CONTROL:

- In this section we will discussed about the database security based on access control. The role based access control method has been proposed by Guoliang Zou, Jing Wang, Dongmei Huang [6] where he has implemented security using the following points:
- Preventing illegal users from logging the system
- Indentify validation
- Access Control Interface
- Verification codes
- Database security: storage procedure
- Database security: oracle parameter

The author Ravi Sandhu has created various security approaches [1] where he has considered that access control policies in early days were based on the development of two different classes of models, the discretionary access control policy and on the required access control policy and procedure. Based on these models of early days [7] have proposed two assumptions:

5.1.1 The first assumption was that the access control models for databases should be defined in terms of the logical data model; hence authorizations for a relational database should be defined in terms of relational model such as relations, relation attributes and tuples etc.

5.1.2 The second assumption is that for databases, in accession to name-based access control, where the secure and protected objects are categorized by giving their names, content-based access control has to be promoted.

Discretionary access control policy has subsidized in the creation and development of System R access control for relational database management system which altered strongly on some key features such as distributed authorization administration, effective grant and revoke of authorizations and the use of views for supporting and developing content-based authorizations. Furthermore the access control policies of an object oriented database (OODBMS) are defined in [8]. Here in this point the author has discussed about two proposed security models for OODBMS. They are given below as:

5.1.2.1 Sorion Security Model: This is a security model proposed by Thurainsingham to associate a secure access control into the ORION model system.

5.1.2.2 Jajodia-Dogan Security Model: Jajodia-Dogan

(6, 12) has proposed a security model for OOBBMS that control access by using the encapsulation characteristic of object oriented database.

Henceforth using the access control policies and procedure the confidentiality of the database can be supported.

The second security issue of database management systems has various fields of database integrity as described in [5]:

Physical database integrity protection: It manages data integrity through physical obstacles such as fires and power failures.

Logical data integrity protection: It refers to the assertion that information is can be changed only by users.

Data element integrity protection: It involves data efficiency and data regularity.

And the third security issue availability as described above belongs to the data availability from the database management system. Henceforth, Due to the availability of company's whole information on the web page which is connected via Internet to its database, the whole data of that company is available using the SQL injection. Thus below section describes the security methods to prevent SQL injection in that scenario.

5.2 SOME SECURITY METHODS TO PREVENT SQL INJECTION

Hence as a protection from SQL injection many Intrusion Detection Systems (IDS) have been suggested. A brief description of these IDS is discussed below:

5.2.1 Misuse Detection System for DBMS

(DEMIDS): This method has been proposed by Chung *et al*. (1999). It is called a misuse-detection system, created for relational databases. It uses audit data log to retrieve profiles describing typical behaviour of users in Database Management System.

The method is present by Lee *et al.* (2000). This method is based on intrusions. Hence this method has used time signatures to discover database intrusions.

On the other way similar work was proposed by Low *et al*.(2002).This method is used for Detecting Intrusion in Databases through Fingerprinting Transactions (DIDAFIT).It is a system created using misuse detection approach to show database intrusion detection at the application level in a database.

But another approach towards a database specific intrusion detection mechanism is by Hu and Panda (2003). They proposed and developed a mechanism that is more capable of finding data dependency relationships among transactions and use this information to find hidden anomalies in a database log. Ke Chen *et al.* (2005) developed an intrusion detection model for a database system based on digital amnesty. It gives an additional layer of security against DBMS misuse.

On other hand a real-time intrusion detection mechanism based on the profile of user roles has been prescribed by Bertino *et al.* (2005). This total approach is based on mining SQL queries stored in audit log files in a database.

Rietta (2006) described an application layer intrusion detection system, which should take the form of a proxy server and apply an anomaly detection model based on distinct characteristics of SQL and the transaction history of a appropriate user application and user.

Aziah Asmawi has proposed SQL Injection and Insider Misuse Detection System (SIIMDS) in 2008 to define both types of intrusions from external and internal threats.

Malicious users may access a series of safe information and then apply different techniques to retrieve sensitive data by using that information. To address this inference problems,Yu Chen in [9] has created a semantic inference model (SIM) that symbolize all the possible inference channels from any attribute in the system to the set of elevated sensitive attributes. Hence based on the SIM, the violation detection system keeps track of a user's query history in a database. When a new query is stiffed, all the channels where sensitive information can be stored will be recognizing. If the probability of inferring sensitive information increased a more specified threshold, then the current query request will be revoked. Using the security methods mentioned in section A and B secure and safe database can be created. It may be accessed from anywhere and the security would be managed.

Even though there is no such thing as a 100 percent guarantee in network security, awful obstacles can be placed in the path of SQL injection attack. Anybody of these defenses extremely reduces the chances of a successful SQL injection attack to prevent our data. Implementing all four is a best practice that will supply high degree of protection and safety. Despite its extensive application, your web site does not have to be SQL injection's next suspect. The next section briefs up all the vulnerabilities, threats and security methods of database management system in tabular format which will be beneficial for the development of secure and safe database. There actually is a lot method that web site owners can do to secure against SQL injection attack.

Table 1. Details of VDBMS, TDBMS and SMDBMS

Vulnerabilities (VDBMS)		**THREATS (TDBMS)**	**SECURITY METHODS SDBMS)**
Vendor Bug	Buffer Overflow, Programming errors	May damage or violate the database	Unauthorized access control policy
Poor Architecture	Weak form of encryption	May damage database environment components (networks, applications, operating systems, DBMS and data)	1.Sorion Security Model 2.Jajodia-Dogan Security Model
Misconfiguration	Not properly locking database	Loss of integrity of the database	1.Physical database integrity protection 2.Logical data integrity protection 3.Data element integrity protection
Incorrect usage	SQL injection	Misuse of availability of database	Intrusion Detection System like 1. A Misuse Detection System for Database System (DEMIDS) 2.SQL Injection and Insider Misuse Detection System (SIIMDS)

			3. Detecting Intrusion in Databases through Fingerprinting Transactions (DIDAFIT) 4. Semantic inference model (SIM)
Irresponsible DBA	Deactivation of necessary security mechanism	Easy access of data	Two principles should be followed: 1. The access control models for databases should be expressed in terms of the logical data model; thus authorizations for a relational database should be expressed in terms of relations, relation attributes, and tuples. 2. For databases, in addition to name-based access control, where the protected objects are specified by giving their names, content-based access control has to be supported.
Hidden Flaws in DB	Undetected defects	Allow hackers to connect to the database server by exploring those defects.	Intrusion Detection System
Unauthorized Users	Unauthorized users "still" the credentials of authorized users	Easy access of database servers.	Intrusion Detection System
Misused Privileges	Authorized users take advantage of their privileges.	Maliciously access or destroy data	Database Administrator should provide security on the basis of above mentioned principles.

6. CONCLUSION

In this paper we have identified the vulnerabilities, threats and security methods of database management system with the help survey conducted on researches of database security. The result of the survey we have described in the paper and summarized in tabular form. As a result we can conclude that though remarkable work has been done in this field, with the invention of internet technology, the risk to database has increased. Many intrusion detection systems for the database have been devised still more research has to be done since there are vulnerabilities in internet connection and website.

7. REFERENCES

[1] Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE, "Database Security—Concepts, Approaches and Challenges" in IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005

[2] Andriy Furmanyuk , Mykola Karpinskyy, Bohdan Borowik, "Modern Approaches to the Database Protection" in IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany

[3] Marco Vieira, Henrique Madeira , "Detection of Malicious Transactions in DBMS", 11th Pacific Rim International Symposium on Dependable Computing

[4] Hassn A. Afyuoni, A Book, "Database security and auditing "

[5] Aziah Asmawi , "System Architecture for SQL Injection and Insider Misuse Detection System for DBMS", my -1-4244-2328 6/08/$25.00 © 2008 IEEE

[6] Guoliang Zou, Jing Wang, Dongmei Huang, LiangJun Jiang, "Model Design of Role-Based Access Control and Methods of Data Security", 2010 International Conference on Web Information Systems and Mining.

[7] E.B. Fernandez,R.C. Summers and C.Wood, Database Security and Integrity. Addison-Wesley, Feb. 1981.

[8] Premchand B. Ambhore,B.B.Meshram,V.B.Waghmare, "A IMPLEMENTATION OF OBJECT ORIENTED DATABASE SECURITY" , Fifth International Conference on Software Engineering Research, Management and Applications.

[9] Yu Chen and Wesley W. Chu, "Protection of Database Security via Collaborative Inference Detection ", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 20, NO. 8, AUGUST 2008

[10] http://www.esecurityplanet.com/hackers/how-to-prevent-sql-injection-attacks.html