International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-5)

Research Article | **May 2015**

Enforcing Database Security in Un-trusted Environment by using Multisession and Biometrics based Authentication

Surya Pratap Singh[1*], Avinash Singh[2], Upendra Nath Tripathi[3]
Department of Computer Science
Deen Dayal Upadhyay, Gorakhpur University
Uttar Pradesh, India

Abstract—

The need of computerisation in every aspect of organization is growing very fast in recent years so as the need of database is also increasing at the same rate. The database as the most valuable resource of today's modern computerization process need to be secured from the improper access and intrusion , because different types of attackers are now trying everything to break the security of the databases. Various methodologies are proposed to help protect the databases from these types of security vulnerabilities but what will happen if the intruder is insider of the organization somehow gain the access of the resources that he do not have right to. So this paper address the key problem incurred in the database security and proposes two mechanisms by which the database can be secured in un–trusted environment.

Keywords— Database security, Insider attack, multisession database authentication, biometrics.

I. INTRODUCTION

The need of database security is very acute in these modern times, as the database is required to store the data of every running application. Every organisation either government, private, social or educational is facing these challenges of database security, because different types of attackers are trying everything to get pass the security of database. So security of the database is of the prime concern in today's modern software development industry and also for all the business industries that uses computer based information.

The term database security is referred to as a method of protecting the confidential and sensitive data which is stored in the repository. It basically works as a protection against any form of illegal access or threat at any level of the database. The database security ensures permitting and denying user actions on database and the contents of the database. All the organizations demand the database to be confidential as they do not want unauthorized access to their data and information. This is the need of the current business industry that the data will also be secured against any malicious or accidental modifications.

There are various aspects in the database security for example security at the conceptual and application layer. The application layer security can be implemented through access control policies but if anyone has the direct access to the database then they can get pass over the access control policies and can perform the malicious activities, so in this way if anyone who fiend the database login and password use in the application can directly modify the database hence cause serious security threats.

II. SECURITY ISSUES IN DATABASE

The database organizations are facing various security issues all of these security leads the database to be vulnerable to different types of security threats. This document represents some of the important security issues of the databases –

A. Deployment Failures

The most important cause of the database vulnerabilities is the lack of care at the moment they are deployed. Although any database is tested for the functional correctness and to assure it is doing what the database is designed to do, but very few testing is done to check the database is not doing things that it should not be doing.

B. Data Leaks

Databases is referred as a "back end " part of the office and secure from Internet- based threats and so as the data doesn't have to be encrypted , but databases also contains a networking interface and so attackers are able to capture this type of traffic to exploit it

C. The Abuse of Database Features

Every database exploits what they have seen based on the misuse of a standard database features. For example, an Attacker can gain access through legitimate credentials before forcing the service to run arbitrary code. In many circumstances this access was gained through simple flaws that allow such system to be able to bypass completely.

D. 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

E. Stolen Database Backups

the attacker might be insider of the corporation who are also likely to steal information contained in the database which is kept in the backups . this is a major security threat to the database because the attacker in this case is insider of the organization.

F. The lack of segregation

The separation of administrator (Database Admin) and user powers, as well as the segregation of duties can make it more difficult for theft and attack undertaken by. This issue is needs to be addressed in early stages of the database design, where the designer has to decide the functionality of the user accounts.

G. SQL Injections

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives.

H. Hopscotch

Rather than using buffer overflow and gaining complete access to a database at the primary level, now the attackers often play a game of Hopscotch for finding a weakness within the architecture that can be used as leverage for more serious attacks until they reach to the database system. For example, an attacker may worm their way through your accounts department before hitting the online transaction (like credit/debit card) processing module.

I. Substandard Key Management

Key management systems are used assure the safety of keys, but we often found that encryption keys stored on company disk drives. DBA sometimes falsely believe these keys have to be left on the disk because of database failures, but placing such keys in an unprotected state cab leads the database system to be vulnerable to attacks.

III. THREATS TO DATABASES

Threats to database may cause the loss of some or all of the security goals –

A. Loss in Integrity – the integrity of the Database refers to the requirement that information be protected from improper modification and alteration. Modification of data includes creation, modification, insertion, deletion and changing the status of the data stored in the database.

B. Loss in Availability – the Availability refers to making objects available to a human user or a program which have a legal access right.

C. Loss in Confidentiality – Confidentiality in database refers to the protection of data from unauthorized disclosure. The unauthorized discloser of confidential information may range from violation of the data privacy act of the geo-faradisation of national security.

IV. REVIEW OF LITERATURE

Various researchers' works on database security some of the important work related to this paper are explained bellow
William G.J.Halfond et al.'s Scheme- [1]- proposed an approach that works by combining static analysis and runtime monitoring of database queries. In its static part, technique uses program analysis to automatically build a model of the legitimate queries that will be generated by the application. While in the dynamic part, the technique monitors the dynamically runtime generated queries and checks them for acceptability with the statically-generated model. A query that doesn't match with the model represent potential SQLIAs and are hence prevented from executing on the database and reported.
Wen-Chung Kuo, Dong-Jin Jiang[2] proposed the block division method and one bit to record the change of the selected minimum point to replace the record data method using in HKC. According to our proposed method and experience analysis, this reversible data hiding scheme is not only to improve the original data hiding capacity but also to reach the goal of data recovering.
Vingralek R – [3] shows that the total memory consumption of GnatDb , which includes the code footprint , the stack and the heap does not exceed 11 KB , while its performance on a typical appliance platform remains at an acceptable level and proposes the methodology by which the memory of database can be made secure.

Iyer B – [4] propose a new secure storage model and a key management architecture which enable efficient cryptographic operations while maintaining a very high level of security. We also assess the performance of our proposed model by experimenting with a prototype implementation based on the well-known TPC-H data set.
Shmueli, Erez [5] reviews related academic work on alternative encryption configurations pertaining to encryption locus; indexing encrypted data; and key management. Finally, the article concludes with a benchmark using the following design criteria: encryption configuration, encryption granularity and keys storage.

V. PROBLEMS IN EXISTING SYSTEM

The database systems become more mature these days as various database researchers and practitioners providing various methodologies of database security. These methods and solutions helps to protect the database from various security issues but none of them is fully able to secure the database from every aspect. Most of the researches are done for the circumstances in which the intruder or attackers are the outsider of the organization, but the attacker may be insider to organization also who intentionally or accidently gain access to the portion of the database for that they do not have access right.

Another problem with the existing system is that the systems till date are based on access control mechanism and most of the systems provide all or nothing method of the user access, if somehow the user logs in to the system then the user can perform malicious transactions and harm the database so there is need to design the multilevel security. The problems in the conventional database are shown in the figure 1.

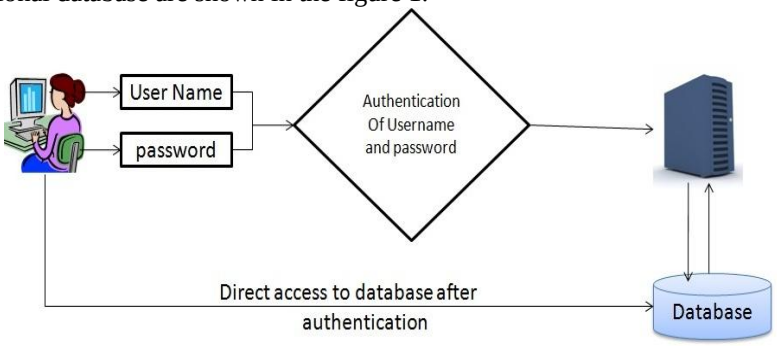

Figure 1.Authintication in traditional database system

Figure 1. shows that if the user enters valid username and password then he/she can directly use the database directly, Because the database authentication module checks for the correctness of the user name and password. But if we use only this scheme of authentication it leads to several problems, like if a valid user tries to do some task that he do not supposed to. For example in an Institution database the librarian is supposed to deal with only books details of the students but if librarian after login start accessing the accounts records of students.

All these scenarios leads us to design a multi level- multi session database authentication module so these problems can be mitigated.

VI. PROPOSED METHODOLOGY

To overcome from the problems we stated earlier we propose the following solutions –

A. Multisession database authentication module – In this approach the login to the database is done in the normal fashion, i.e. it is done in the same way as in case of traditional database but the login in valid for a definite session. When the user log in the database by providing valid username and password the he/she allowed to use the system resources but for a finite period of time so when the timer expires the user are prompted to enter the password again if the user provides valid password the login continues as normal but if any deviation found the system triggers an alarm. This way we protect the database from the situations in which if the valid user left the database in login mode and somehow an intruder uses that system from malicious activity. This method is explained in the figure 2. Given bellow.

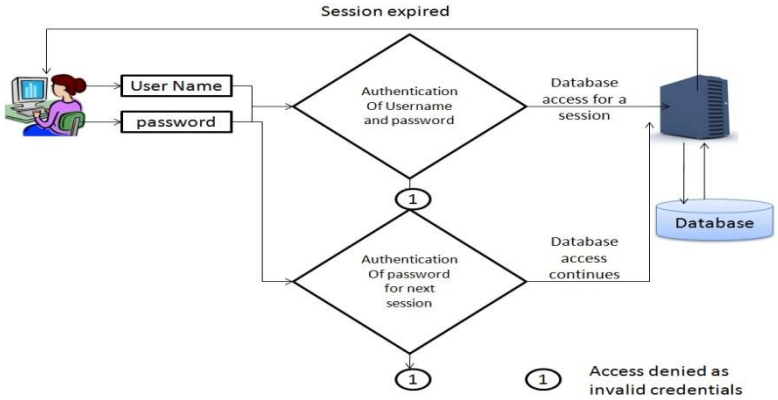

Figure 2.Database security By Multisession database authentication module

B. Biometrics based Transaction level authentication – In this approach the user login to the database by providing user name and password along with the biometrics credentials. The privilege of the user to use system resources and perform actions are also controlled by the role the user plays in the database and the access rights and privileges are defined for the user at the time of creation of the database account for the user by Database Administrator. To ensure the database security we use two approaches –

i. In first approach we propose the use of statistical role based access monitor. This module records the statistical data about the use of database in normal conditions. When the user tries to perform some operations it is matched with those stored in the statistical role base access monitor, if any deviation found then the system triggers an alarm and abort the operation of the of the user. In this way ensure the valid database user cannot perform the operations that he do not have right to.

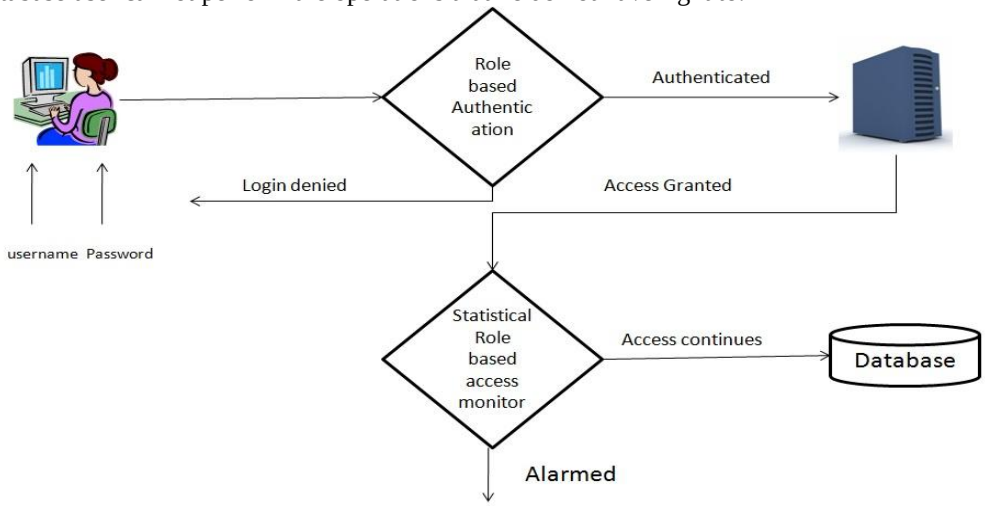

Figure 3.use of Statistical role based access monitor

ii. In second approach we propose the use of biometrics based verification of the transaction the user perform on the database. When the valid user login earlier wants to perform some transactions to the database then he/she have to pass the biometrics credential to commit the transaction. For this purpose the biometrics credentials of each valid user is stored in the database and when the user tries to commit the transaction then he have to pass the biometrics credential and it is matched with those stored in the database.

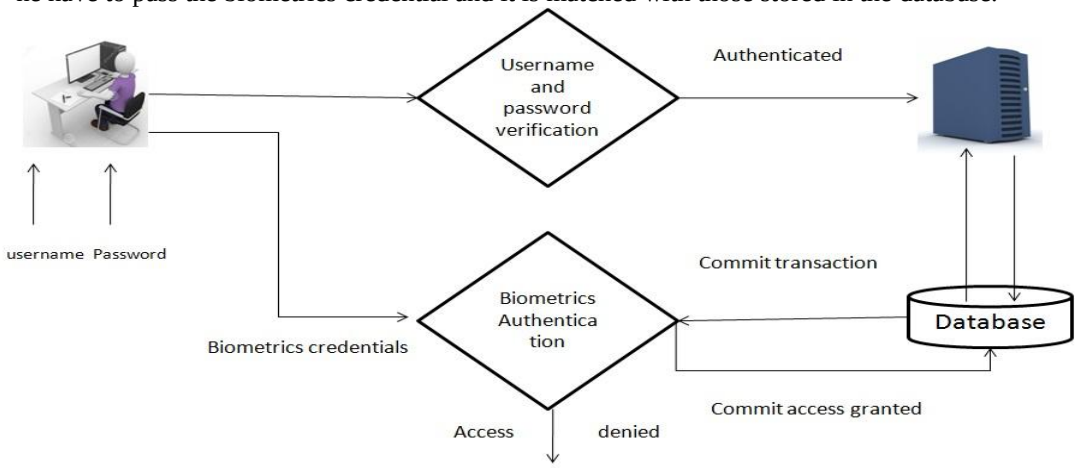

Figure 4.Use of Biometrics based transaction verification.

From the above approach we can –

a. Identify the user who is responsible for the database transaction to commit
b. Prevent the database from unauthorized and un privileged transaction processing.

VII. CONCLUSIONS

the database security is very important in today's environment, as the database attacks are growing very fast .the malicious transaction and improper use of database if any compromise the overall database security. By this way any intruder can gain access to the database of those resources that he/ she is not supposed to, and harm to the database contents so there is need of extensive security in the database system by which any attempt of the improper use of the database can be prevented. There are various approaches to overcome from these security issues but none of them are fully able to protect the database from all types of security issues the database might have. The serious issue with the database security is that if the valid user of the system misuses the database to do the malicious activity.

So, in this paper we explain various security issues the database might have and proposes two approaches , use of multisession authentication module and biometrics based transaction level security to overcome from these problems.

REFERENCES

[1] William G.J.Halfond and Alessandro Orso ―AMNESIA:Analysis and Monitoring for Neutralizing SQL-Injection Attacks

[2] Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, ―A Reversible Data Hiding Scheme Based on Block Division‖, Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369..

[3] Vingralek R (2002) Gnatdb: A small-footprint, secure database system. The 28th Int'l Conference on Very Large Databases, Hong Kong, China, August, pp. 884-893.

[4] Iyer B, Mehrotra S, Mykletun E, Tsudik G, Wu Y (2004) A Framework for Efficient Storage Security in RDBMS. E. Bertino et al. (Eds.): EDBT 2004, LNCS 2992, pp. 147-164.

[5] Shmueli, Erez, Vaisenberg, Ronen, Elovici, Yuval and Glezer, Chanan(2009)Database Encryption- An Overview of Contemporary Challenges and Design Considerations SIGMOD Record vol38, No 3.

[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.

[7] Karlsson, J. S.: Using Encryption for Secure Data Storage in Mobile Database Systems. Friedrich-Schiller-Universidad Jena. (2002).

[8] Bertino E, Ferrari E (2002) Secure and Selective Dissemination of XML Documents. ACM Transactions on Information and System Security, 5(3), 290-331.

[9] He J, Wang M (2001) Cryptography and Relational Database Management Systems, Proceedings of IEEE Symposium on the International Database Engineering & Applications, Washington, DC, USA.

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

[11] www.wikipedia.com

[12] C. Gould, Z. Su, and P. Devanbu. Static Checking of Dynamically Generated Queries in Database Applications. In Proceedings of the 26th International Conference on Software Engineering (ICSE 04), pages 645–654, 2004.

[13] Roichman, A., Gudes, E.: Fine-grained Access Control toWeb Databases. In: Proc. of 12th SACMAT Symposium, France (2007)

AUTHOR'S PROFILE

Surya Pratap Singh is MCA and UGC-NET qualified and pursuing Ph.D. In the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Database Security, Networking. Mr. Surya Pratap Singh has published 12 papers in different national and international conferences/ Journals.

Avinash Singh is M.Sc. Computer Science, M.Tech and M. Phil and pursuing Ph.D. in the department of Computer Science DDU Gorakhpur University, Gorakhpur (U.P. India) under the supervision of Dr. U.N. Tripathi. The area of research interest is Database Security, Networking. Mr. Avinash Singh has published 22 papers in different national and international conferences/ Journals.

Dr. Upendra Nath Tripathi is Assistant professor in Department of computer science DDU Gorakhpur University, Gorakhpur (U.P. India). He has 13 years of teaching and research experience. He has published 46 papers in various National and International Journals/conferences. His area of research interest is database systems, networking.

