Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Database Szecurity Threats

Manisha Sharma
Assistant Professor, Department of Computer Science & Technology, Hindu Kanya Mahavidyalaya, Dhariwal, Punjab, India

Abstract: The basic problems are access control, exclusion of spurious data, authentication of users and reliability. In this paper the challenges and threats in database security are identified. Database security strives to insure that only authenticated users perform authorized activities at authorized times. While database security incorporates a wide array of security top-ics, notwithstanding, physical security, network security, encryption and authentication, this pa-per focuses on the concepts and mechanisms particular to securing data. The basic problems are access control, exclusion of spurious data, authentication of users and reliability. In this paper the challenges and threats in database security are identified.

Keywords: Attack, Database security, Threat, Integrity.

I. INTRODUCTION

Database security is a series of processes and systems which are put in place to protect the database items from any outside alein that has a poor intent or from anyone inadvertently accessing the database, whether they may be authorized or not authorized. There are many security measures in place such as firewalls, antivirus and routers, and these are some examples of those handling the external security of the database. Database security is a growing concern evidenced by an increase in the number of reported incidents of loss of or unauthorized exposure to sensitive data. 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].

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 [2]:

D. 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.

E. 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]:

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 [6], 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 [6].

III. SETTING UP THE DATABASE SECURITY

The Database security placed in a database can begin by the construction of a set security standard placed in the environment of the database. It included in the database standard are the controls for different platforms and links. Authentication as well as integrity is also part of the security procedures placed in a database.It is the duty of the administrators of the database is to check for vulnerability. This is done to see whether is there are holes in the system that can allow other sources into the database

IV. REAL-TIME MONITORING

It is very important that the real-time monitoring of the database that allows the administrator to monitor the ways usually used to access the database, this is done so as they can gather or have an idea of any unrecognized movement within this path to the database. This will help eliminate possible sources or unauthorized users to access the database.

V. SECURITY ISSUES IN E-COMMERCE DATABASES

An e-commerce system is a trading platform which sets up in a more open network environment. The transaction process is broadly divided into user registration, user login, purchasing merchandise, online payment and so on. When user information is transmitted in the web it may be stealed by hackers or other people with ulterior motives and will result in property loss. Therefore ensuring the security and integrity of basic information of users is the basis for the smooth conduct of e-commerce.[1]

VI. ACCESS CONTROL – GRANT/REVOKE

Access control is a core concept in security. Access control limits actions on objects to specific users. In database security, objects pertain to data objects such as tables and columns as well as SQL objects such as views and stored procedures. Data actions include read (select), insert, up-date, and delete or execute for stored procedures. For instance a faculty member, Dr. Smith, may be given read privileges to the Student table.

Generally, access control is defined in three ways: Mandatory Access Control (MAC), Discre-tionary Access Control (DAC), and Role Based Access Control (RBAC). MAC and DAC provide privileges to specified users or groups to which users are assigned. MAC rules are system applied and considered static and more secure. An example MAC rule would be giving Dr. Smith read access to the Student table. DAC rules are user supplied, considered dynamic and content fo-cused. An example DAC rule would be giving Dr. Smith read access to the Student table but only for students enrolled in a specific course such as 'Introduction to Security.' Dr. Smith would not be able to select student data for students enrolled in other courses. MAC and DAC provide pow-erful tools but Role Based Access Control proves to be especially effective for database systems. Roles are analogous to job functions. With roles, the focus is on identifying operations and the objects to which those operations need access. Users assigned to a role automatically receive its associated privileges. For instance Dr. Smith may be assigned to the role of Faculty. Faculty members are given rights to read the Students table, obtain course enrollment data, and update grades for students assigned to their courses. By being assigned to the Faculty role, Dr. Smith is implicitly given these privileges.

Identifying users and assessing their processing and data access needs is a major undertaking in establishing good database security protocols. Identifying and defining roles and correctly grant-ing access rights to actions and objects and then appropriately assigning users to those roles is the crux of the process. Once a role has been created, the format for implementing RBAC follows the pattern:

GRANT privilege_name
ON object_name
TO role_name;

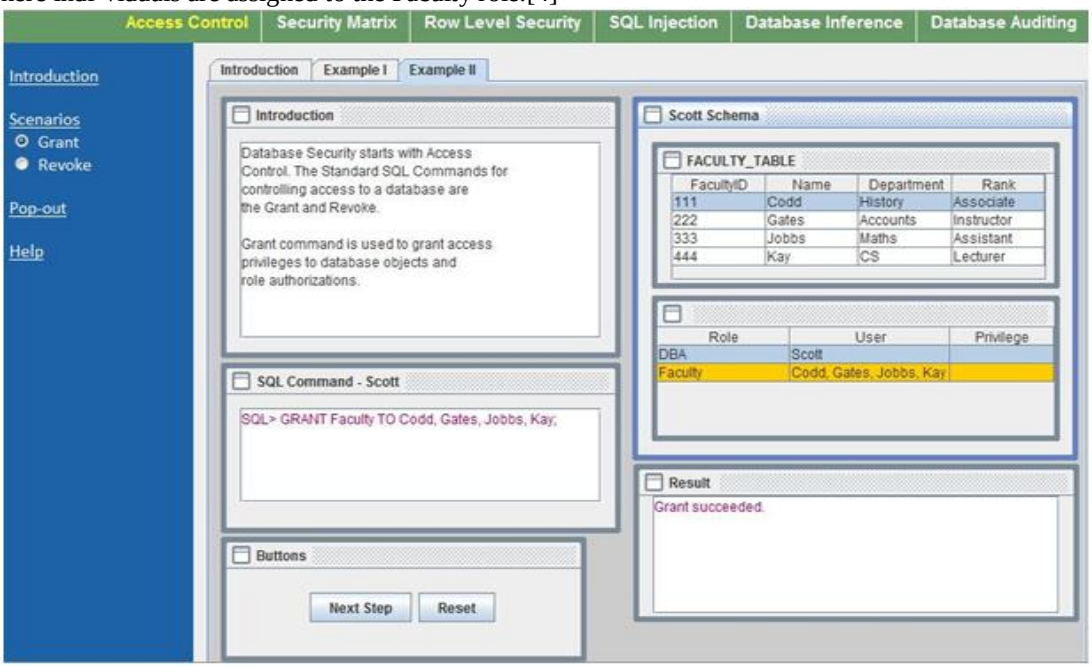
Privilege_name identifies the rights to be granted. These include such rights as selecting data, modifying data, or manipulating the database structure. ON identifies the database objects and TO identifies the roles to which those

privileges are applied. For instance, if Dr. Smith was as-signed the role of Faculty and Faculty were given read rights to the Student table, the RBAC rule would be:

GRANT Select
ON Student_Table
TO Faculty;

The Access Control sub-module on the ADbC site introduces the concept of access control and provides two examples for granting and revoking privileges. The introduction explains the proc-ess and models its implementation through corresponding SQL statements. Example one uses a student scenario and example two uses a faculty scenario. The grant sub-module steps through the process of assigning users to roles and assigning privileges to those roles. For example, using the faculty scenario, the steps for granting role authorization to individual users include having a da-tabase administrator create the role of faculty, assigning faculty to this role, and then assigning specific rights or privileges to database objects.

After being assigned to the role of Faculty, the user has all privileges assigned to that role. Figure 1 depicts the step in the process where indi-viduals are assigned to the Faculty role.[4]



VII. CONCLUSION

Security is an important issue in database management . The data in a database management system need to be protected from abuse and should be protected from unauthorized access and updates By using hybrid encryption technology can give full advantages of two kinds of encryption algorithm and provides more reliable and efficient security for database. Database security is becoming an increasingly important topic and students need to develop core understandings in this area. This paper suggested a set of sub-topics in a database security course component and introduced a set of interactive software modules mapped to each sub-topic presented.

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

[3] ISBN 978-952-5726-00-8 (Print), 978-952-5726-01-5 (CD-ROM) Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)*Nanchang, P. R. China, May 22-24, 2009, pp. 363-366*

[4] Journal of Information Technology Education:Volume 9, 201 ,Innovations in Practice,*Meg Coffin Murray,Kennesaw State University, Kennesaw, GA, USA.*

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

[6] http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0309.pdf

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

