***Security in Database Systems***

Mohit Sunil Sajnani

Department of Computer Engineering

VESIT-Chembur

Mumbai, India

2015mohit.sajnani@ves.ac.in

*Abstract* — In today's world, data is generated at a very rapid speed and final destination of such data is database. Data is stored in database for easy and efficient way to manage these data. All the operations of data manipulation and maintenance are done using Database Management System. Considering the importance of data in organization, it is essential to secure the data present in the database. A secure database is the one that is reciprocated from different possible database attacks. Security models are required to develop for databases. These models are different in many aspects as they are dealing with different issues of the database security. In this paper, I have discussed some of the attacks that can be possible with its counter measures and its control methods that can be possible. Securing database is important approach for the planning of explicit and directive based database security requirements. Ensuring security for database is very critical issues for the companies. As complexity of database increases, we may tend to have more complex security issues of database.

# Introduction

A database can be defined as a collection of data that is saved on a computer system’s hard drive. Databases allow any authorized user to access, enter and analyze data quickly and easily. It is a collection of queries, tables and views. The data stored in the databases are usually organized to model aspects that support processes that require information storage and retrieval. Major chunk of data are stored in the repository called database. The user interface for databases is called a database management system. DBMS are a software application that interacts with the authorized user, other applications and the database itself to capture and analyze data. It helps to organize data for better performance and faster retrieval by maintaining indices. DBMS performs the function of concurrency control. DBMS also performs data recovery operations of database. Now a day’s enterprises need databases to store any type of data needed, because of the speed and affordable cost database is popular among the enterprises. Advantage of using the database is it automates different procedures, saving resources and person-hours. For example, instead of manually verifying transactions, users can rely on computer reports stored in the database. Instead of entering warehouse or retail stock information manually, hand held scanners could be used to save information in the database. A database can provide efficiency and speed in the modern workplace. Next question for any organization is “Is Data secured using database?” Security in today’s world is one of the important and challenging tasks that people are facing all over the world in every aspect of their lives. Databases are complex and many database security professionals do not have full understanding of risk and security issues related to different databases.

# Traditional database security

Security in SQL = Access control + Views

Security in statistical databases = Theory

1. Access Control in SQL:

GRANT privileges ON object TO users [WITH GRANT OPTIONS]

Privileges = SELECT | INSERT | DELETE | . . .

Object = table | attribute

REVOKE privileges ON object FROM users [CASCADE]

1. Views in SQL:

A SQL View = (almost) any SQL query

Typically used as:

CREATE VIEW tmpStudents AS SELECT \* FROM Students WHERE…

GRANT SELECT ON pmpStudents TO Sam

1. Summary of SQL security:

It has many limitations such as no row level access control; table creator owns the data and only 30% assign privileges to users/roles, most policies in middleware: slow, error prone. Today the database is not at the center of the policy administration universe.

1. Statistical database security:

The goal of statistical database security is to allow arbitrary aggregate SQL queries and hide confidential data. Query restriction, query-size control, query-set overlap control, query monitoring have been tried but none of them is practical. Original goal seems impossible to achieve and cell combination/suppression are popular, but do not allow arbitrary queries.

# database security threats and counter-measures

* Excessive Privileges: Privileges of database can be abused in many ways. User may abuse privilege for unauthorized purpose. Privilege abuse comes in different flavors: Excessive privilege abuse, legitimate privileges abuse and unused privilege abuse. This type of threat is most dangerous because authorized users are doing misuse of data. These privileges can be abused and creates unnecessary risk. Granting excessive permissions is problematic for two reasons. About 80% of the attacks on company data are actually executed by employees or ex-employees. Granting too many privileges or not revoking those privileges in time makes it unnecessarily simple for them to execute their wrongdoing. Some of these actions might even be executed inadvertently or without the perception of those actions being illegal.

Counter-measures: Access Control policy: Do not grant unnecessary privileges to the user.

Legitimate privilege abuse can be stop by a providing good audit trail.

* SQL Injections: Database systems are used for the backend functionality. User supplied data as input is often used to dynamically build SQL statements that affect directly to the databases. Input injection is an attack that is aimed at subverting the original intent of the application by submitting attacker –supplied SQL statements directly to the backend database. There are two types of input injection: 1. SQL Injection 2. NoSQL Injection.SQL Injection: Targets the tradition database system. It attacks usually involve injecting unauthorized statements into the input fields of applications. NoSQL Injection: Targets big data platforms. This type involves inserting malicious statements into big data components like Hive, Map Reduce. In SQL and NoSQL successful input injection, attack can give an attacker unrestricted access to an entire database.

Counter-measures: Use Stored Procedure instead of implementing direct queries and implementing MVC Architecture.

* Malware: Cybercriminals, state-sponsored hackers, and spies use advanced attacks that blend multiple tactics – such as spear phishing emails and malware – to penetrate organizations and steal sensitive data. Unaware that malware has infected their device; legitimate users become a conduit for these groups to access your networks and sensitive data. Counter-measures: Enable firewall protection and Install Antivirus.
* Weak Audit Trial: Weak audit policy and technology represent risks in terms of compliance, deterrence, detection, forensics and recovery. Automated recording of database transactions involving sensitive data should be part of any database deployment. Failure to collect detailed audit records of database activity represents a serious organizational risk on many levels. Organizations with weak database audit mechanisms will increasingly find that they are at odds with industry and government regulatory requirements. Most audit mechanisms have no awareness of who the end user is because all activity is associated with the web application account name. Reporting, visibility, and forensic analysis are hampered because there is no link to the responsible user. Finally, users with administrative access to the database, either legitimately or maliciously obtained, can turn off native database auditing to hide fraudulent activity.

Counter-measures: Network-based audit appliances are a good solution. Such appliances should have no impact on database performance, operate independently of all users and offer granular data collection.

* Backup Exposure: Backup storage media is often completely unprotected from attack. As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect backup copies of sensitive data and monitor your most highly privileged users is not only a data security best practice, but also mandated by many regulations.

Counter-measures: Encrypt Databases: Store data in Encrypted form as this allows you to secure both production and backup copies of databases, then audit the activity of and control access to sensitive data from users who access databases at the operating system and storage tiers. By leveraging database auditing along with encryption, organizations can monitor and control users both inside and outside of the database.

* Weak Authentication: Weak authentication schemes allow attackers to assume the identity of legitimate database users. Specific attack strategies include brute force attacks, social engineering, and so on. Implementation of passwords or two-factor authentication is necessary. For scalability and ease-of use, authentication mechanisms should be integrated with enterprise directory/user management infrastructures.
* Denial of Service: In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Counter-measures: Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping. Ensure that the software and protocols used are up-to-date and scan the machines thoroughly to detect any anomalous behaviour.

# Conclusion

Organizations now are relying on data to make decisions on various businesses operations that enhance their operations. Therefore, it is prudent to keep sensitive information away from unauthorized access. The above research paper has attempted to explore the issues of threats that may be poised to database system. These include loss of confidentiality plus loss of integrity. Besides, it has detailed on loss of privacy leading to blackmail and embarrassment in the business. The paper has also discussed areas concerning techniques to counter any issue of threat. These could be use of views and authentication. Another method is through back-up method that ensures that the information is stored elsewhere and recovered in case of failure or attacks. The paper has also discussed the requirements that are set for a robust database management system. Some of the requirements are audit trial. Lastly, the paper has looked at the process for managing a database system and has discussed all the steps that need to be taken.

# references

1. Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers, 2005.
2. S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
3. S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
4. Implementing database security and auditing, Ron Ben Natan.
5. Shelly Rohilla, Pradeep Kumar Mittal, and Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
6. Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015