**Assignment 11 - Research and Review of Security Issues**

**Review of the papers and the main issues addressed by them:**

Database security is a vast module and some concepts related to database security and their corresponding submodules are covered in this paper. The submodules cover six areas, and they are: access control, row level security, application security as portrayed in a security matrix, SQL injections, database inference, and database auditing and these six modules are briefly discussed. This paper [1] discusses security challenges such as protection of data from unauthorized disclosure, prevention from unauthorized data access, identification and recovery from malicious activity resulting in the denial of data availability. The author in [1] has justified the reason for not including all the relevant sub-topics for database security, the focus is limited to mechanisms for securing data, hence only five modules were included.

The author defines access control as a way to restrict access to the system by assigning rights and privileges to specific data objects and data sets in combination with authentication and authorization; the author then sheds light on three ways of defining it: Mandatory Access Control (MAC) Discretionary Access Control (DAC), and Role-Based Access Control (RBAC). The article then describes Application Access Management and explains how a security matrix can visually help in identifying the correlation between the operations performed on a database and the authorizations needed for database objects. The author has further highlighted that visual depiction of data integrity rules makes it easy to identify all application programs potentially affected by any change made to a database table.

Paper [1] discusses Database inference as the ability to infer unknown information from retrieved information. It states that inference often happens in cases where the actual intent is for users to generate or view aggregate values when they have not been given access to individual data items. The author has stressed that there are no ideal solutions to Database Inference. The author of paper [1] seeks to establish database auditing as a way to identify if breaches have occurred rather than preventing the breach itself. The author categorizes audits as an activity tracker for Data Control Language, Data Definition Language, Data Manipulation Language, and logon/logoff attempts. The author described one of the solutions to the above problems were to incorporate a set of interactive software modules referred to as Animated Database Courseware (ADbC) to support the teaching of database concepts as a means of reinforcement learning for students.

The second paper [2] listed below in references discusses a comprehensive approach for data protection such as adding mechanisms for enforcing access control policies based on data contents, subject qualifications and characteristics, and other relevant contextual information, such as time to already existing techniques such as encryption and electronic signatures. The paper [2] also talks about several new challenges faced by database security such as disintermediation access to data, security concerns, computing paradigms and applications etc. This paper also discusses the most relevant concepts of database security and summarizes the most well-known techniques. It focuses on access control systems, describes the key access control modules, security for advanced data management systems and access control for XML.

The paper [2] discusses security breaches and their categories such as unauthorized data observation, incorrect data modification and data unavailability. Unauthorized data observation leads to disclosure of information to unauthorized users. All organizations especially healthcare and security may suffer losses both financially and human point of view because of unauthorized data access. Incorrect data modifications intentionally or unintentionally lead to databases being in incorrect state. The use of data when the database is in incorrect state leads to heavy losses for the organization. When data is unavailable, information crucial for the proper functioning of the organization is not readily available when needed.

Paper [2] suggests that the complete solution for database security must meet the following three requirements:

1) secrecy or confidentiality:

 refers to the protection of data against unauthorized disclosure.

2) integrity:

 refers to the prevention of unauthorized and improper data modification.

3) availability:

 refers to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system unavailable.

The paper [2] discusses database protection and the different components that ensure database protection and in particular access control mechanisms that ensure data confidentiality. Access control mechanism checks the rights of the user against a set of authorizations (States whether a subject has access to the particular object or action) usually stated by the security administrators.  It also discusses what each database technique does like. It states that Recovery subsystem and concurrency control mechanism ensures the data is available and correct despite hardware and software failures, implementing techniques to protect against DoS attacks can strengthen data availability.

Several emerging research in databases such as recent research direction motivated by the trend of considering databases as a service that can be outsourced to external companies, other important issues such as development of query processing techniques for encrypted data, several specialized encryption techniques such as the orderpreserving encryption technique were discussed in the paper [2].

The paper [2] also talks about privacy-preserving techniques for databases. It states that Research in this direction has been motivated, on one side, by increasing concerns with respect.

to user privacy and, on the other, by the need to support Web-based applications across organization boundaries.

**How are the two articles connected?**

With the rise of web-based applications and increasing growth in databases, providing appropriate security is the prime concern. The aim of both the papers is to recognize security concerns and provide approaches to ensure a controlled, protected access to databases and in the process, preserve the integrity, consistency, and overall quality of data. Both the papers provide approaches that can be implemented to secure the database from unauthorized access and possible data breaches.

**Three key takeaways from the two articles listed below:**

1. The security of any database can be improved but it likely degrades the performance. If we try to increase the performance of the database along with the security, the cost to maintain the database increases. In other words, there exists a tradeoff between performance, security, and cost.
2. CRUD (Security Matrix) can be used to explicitly identify the access rights required by the application program. It also provides visual depiction of the correlation between the authorizations needed for the database objects and input/output sources such as forms and reports.
3. To protect data and prevent data breaches, always make sure to change default credentials, review user account privileges, avoid sharing credentials, enable application logs, monitor application logs, perform code reviews and application tests to avoid SQL injection.

**Are there statements that you do not agree with?**

I agree with the statements presented in both articles. No matter how many security measures are available, database security is a constant concern. As security keeps increasing, attacks too are getting smarter hence we need to keep working on database security to ensure the data can be kept safe and protected.

**References:**

[1] Murray, M. C. (2010). Database security: What students need to know. Journal of information technology education: Innovations in practice, 9, IIP-61.

[2] Database Security—Concepts, Approaches, and Challenges, Elisa Bertino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE