Assignment 7 – Research and Review of Security Issues

Name: Saisrihitha Yadlapalli

Review and main issues addressed:

Database security is a vast concept and some of the important constructs and mechanisms particular to securing data have been discussed in [1]. This paper enables students to understand 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 solutions to these problems were well explained by incorporating 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.

[2] covers the viewpoint of forensic investigators on one of the largest data breaches in history with a goal to ensure that the analysis and findings presented prove to be helpful in the planning and security efforts to avoid such breaches in the future.

Moreover, their findings provide an insight into who commits these acts and how they occur. They have found that most data breaches originate from external sources, with 75% of the incidents coming from outside the organization as compared to 20% coming from inside. They also report that 91% of the compromised records were linked to organized criminal groups. Further, they cite that the majority of breaches that result from hacking and malware are often facilitated by errors committed by the victim, i.e., the database owner. ***Unauthorized access and SQL injection*** were found to be the two most common forms of hacking, an interesting finding given that both of these exploits are well known and often preventable. Given the increasing number of breaches to database systems, there is a corresponding need to increase awareness regarding efforts to properly protect and monitor database systems.

Some of these efforts are discussed in [1] as follows:

- **Access control:** The process by which rights and privileges are assigned to users and database objects. (grant/revoke and row-level security)
- **Application access:** Addresses the need to assign appropriate access rights (using security matrix) to external applications requiring a database connection.
- **Vulnerability inference:** Refers to weaknesses that allow malicious users to exploit resources. Inference refers to the use of legitimate data to infer unknown information without having the rights to directly retrieve that information. A possible solution to this inference problem is poly-instantiation.
- **Auditing mechanisms:** Auditing is not a prevention method, but it tracks database access and user activity providing a way to identify breaches that have occurred so that corrective action can be taken.

Now, let us consider one of the most used data breaching technique - **'SQL injection'**. As per the statistics presented in [2], 79% of the records were breached in 2008 using this. At its most basic level, SQL injection attacks exploit a failure to properly validate user input and is common with custom-developed applications and web front-ends. Secure development, code review, application testing, etc. are considered beneficial in light of this finding. This situation could have been avoided by using the below security measure discussed in [1].

SQL injections can be prevented by validating user input. The importance of input validation cannot be overstated. It is one of the primary defense mechanisms for preventing database vulnerabilities, especially SQL injections. The following three approaches are commonly used to address query string validation:

- **Black list:** Parses the input string comparing each character to a predefined list of non-allowed characters.
- **White list:** Approach is similar except that each character is compared to a list of allowable characters.
- **Parameterized queries:** Uses internally defined parameters to fill in a previously prepared SQL statement.

How are the two articles connected?

With the increasing growth in database, providing appropriate security is the prime concern. The aim of both the papers is to recognise security concerns and provide different approaches to ensure a controlled, protected access to database contents and in the process, preserve the integrity, consistency and overall quality of data.

The analysis presented in [2] establishes the importance/need for database security and serves as an insight to identify specific problem areas common to many organizations and helps to accordingly employ the most suitable combination of database security solutions presented in [1] that would effectively secure the data and prevent any possible data breaches in the future.

Three key takeaways:

1) Unauthorized access via default, shared, or stolen credentials is one of the most common data breaching method. However, I have come to understand that this attack is one of the easiest to mitigate by employing the right access control mechanisms. This can be done through authentication (username and password), authorization (assigning defined privileges) and access control (assigning rights to specific data objects and data sets).

2) I've learnt that the following strategies are key to protect data and prevent data breaches:
    - Changing default credentials.
    - Avoiding shared credentials.
    - Reviewing user account privileges on a regular basis.
    - Application testing and code review to avoid SQL injection and cross-site scripting attacks.
    - Enabling application logs and monitoring them.

3) Lastly, I have inferred that the security of any database can be improved. However, it likely degrades the performance of the database and increases the cost to improve database security while maintaining database performance. That is, the trade-off consists of three axes - performance, security, and cost.

Are there statements that you do not agree with?

I agree with the statements presented in both articles. I would like to point out that no matter how many security measures are available, database security is a constant concern. As security keeps increasing, attacks too are getting smarter. However, [1] fails to mention the scope of incorporating security measures, i.e., if all strategies need to be implemented or only a few will do, if so then what would be the deciding factor to choose one over the other. In [2] the author suggests that the same security breaches are occurring over and over again even with knowledge of security techniques and strategies to prevent them, but no explanation has been given as to why this is happening.

References of the reviewed papers:

[1] **Primary paper:** *Murray, M. C. (2010). Database security: What students need to know. Journal of Information Technology Education: Innovations in Practice, 9, 61-77. Retrieved from http://www.jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf*

[2] **Report referenced by primary paper:** *Baker,W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., Tippett, P., & Valentine, J. A. (2009). The 2009 data breach investigations report. Verizon Business. Retrieved January 31, 2010, from* https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/2009_databreach_rp.pdf