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

[2] - *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 http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf*

Introduction

With the increase in growth of databases, providing appropriate security is the prime concern of any database system. The aim of both the papers is to recognise security concerns and provide different approaches to have a controlled, protected access to the contents of your database and, in the process, preserve the integrity, consistency, and overall quality of your data. Insights of the breaches from [2] can help to decide and implement the required security mechanisms to prevent further attacks. Some of these security techniques have been presented in [1].

Summary

The paper [1] discusses different approaches presented to securing data and [2] provides an insight into the statistics of the number and type of breaches occurring. Using the information about sources of the breaches, how they occur, attack category, etc., would be very insightful in preventing future security attacks. One such example to provide a understanding on how the information about the breaches can be used to enhance the security solution is discussed here- Taking one of the findings of the Verizon Business Risk Team on the 'Source of data breaches' it can be seen that most data breaches originate from external and internal sources. With proper access control implementations presented in this paper, we can minimise the number of breaches occurring externally as there will be authorization and authentication of a user like username passwords to restrict the access. Additionally, specific users can be granted only certain privileges, this can be achieved using the grant/revoke access control mechanism. Further the paper also states the importance of creating views of different tables and how they can be used to provide a more granular access on the rows and columns that are allowed to be visible to a particular user. Through the proper implementation of access control, security risks from external source and internal unauthorized sources can be reduced and data can be protected. Implementing this will help mitigate unauthorized access to users which would result in a data breach.

Similarly, the report also shows that in most of the successful breaches, the attacker exploited some mistake committed by the victim, hacked into the network, and installed malware on a system to collect data. Out of these, SQL injections were the top hacking technique. SQL injections occur in dynamically created user input where the input tricks the database into thinking is the valid input. The vulnerability occurs primarily because of the features of the SQL language that allow embedding comments, concatenating SQL statements just by separating them using semicolons, and the ability to use data dictionaries to query metadata. The paper states that the only way to prevent a SQL injections is by validating user input. Three

approaches for validation are achieved by using black list, white list, or implementing parameterized queries are presented in the paper.

Apart from various access control mechanisms, the paper also discusses about the database interference and auditing. Interference is the ability to derive secure unauthorized information through the combination of other information retrieved which would help to decipher the confidential data. Whatever the sophistication and aggressiveness of attacks, the ability to detect a breach when it occurs is a huge stumbling block for most organizations. Auditing helps to keep a track of database access and user activity, what actions was performed and what data was changed. Auditing is not a prevention method but only used for identifying. The real challenge with database auditing is that we need to know how much data needs to retained and for how long.

Conclusion and Critical questions

We can find that security breaches are a result of a series of intertwined and orchestrated events, Examining the frequency and trends of them would be essential for determining the right security control to be applied. The Verizon Business Risk Team, who have been reporting data breach statistics since 2004, examined 90 breaches during the 2008 calendar year. They reported that more than 285 million records had been compromised, a number exceeding the combined total from all prior years of study.Their findings provide insight into who commits these acts and how they occur. Given the increasing number of beaches to database systems, there is a corresponding need to properly implement and monitor database systems.

However, I would like to point out that no matter how many approaches we take up, the security is a constant concern. As we keep improving the security of the database, even the attacks are getting smarter and better. The author of the paper has introduced the important security topics and their usefulness. However, the paper fails to mention the scope of incorporating the security techniques provided into our database system. Do we need to apply all the security techniques or only a few strategies, if only a few of them are incorporated then what would the deciding factor for implementation be. From the trend in data we can clearly note that similar kind of attacks are repeated over and over but no explanation is given in either of the papers on why we are still facing similar breaches even with the knowledge on database security techniques. Additionally, if a database hacker has access to admin credentials, the audit data could be erased, so in my opinion, the auditing of data is not very significant to trace and identify if breaches have occurred since it can also be easily compromised if the overall security is weak.

Apart from the different techniques to security implementation we also need to consider the following recommendations given by the Verizon Business team which are missed out by the author:

- Ensuring that the policies set up for security are constantly followed, it needs to be an integral part of every organisation and database to incorporate and follow through.
- Ensure to change the default credentials: More criminals breached corporate assets through default credentials than any other single method in 2008.

Points I learn from reading this paper are:

- Ability to achieve row level security by using views
- What are SQL injections and how exactly they occur. Also, the three approaches to prevent SQL injections by validation input data: black listing, white listing and parameterised queries
- Different sources of a breach, different types of possible threats, and types of errors resulting in a compromise of security.