Database Security - Today's Concern

Prassana Shivputra Pailwan

Student, Computer Engineering Department, K.E. Society's Rajarambapu Institute of Technology,
Sangli, Maharashtra, India

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 10, Issue 5, September-October 2022

Abstract
In daily life, the use of technology is increasing as it is making the life of humans easier and more efficient. One such important technology is database. Big firms and MNCs use databases to store data to keep it intact and easy to retrieve. Database stores important information about major assets of the company and it needs to be confidential. The study was conducted to identify and address the issues and threats in databases, requirements for database security, and the level of security which should be provided.

Keywords: Database Management System, DBMS, Computer Security, Cyber Threats, Cyber Security

1. Introduction

Database security deals with the tools and controls to maintain and preserve the database properties - confidentiality, integrity and availability. Security is very important from every perspective. A company or a firm should implement security to run things properly. If it leads to an attack, the data might be lost or can be misused. As a database may contain very sensitive information, which is vulnerable to crackers, nowadays companies have great control and check on their database to maintain its integrity; systems are under surveillance to avoid attack and maintain security. If the data integrity is lost, it may lead to issues in accessing data efficiently, as well as a huge loss can occur and affect the company severely. Another major problem is confidentiality; if it is lost then it may lead to a big problem, as it may be accessed by any cracker. If database privacy is lost then it may be used for blackmailing. Database should be secured with confidentiality, integrity and availability.

1.1. Why Security is Important?

Security is important in today’s world because data is money. If it is leaked or lost, it can harm an organization in many ways; like, it can affect the reputation of the organization, it can affect finances. So all MNCs and big organizations have a special team for security purposes.

2. Database Security and Threats

Database security issues may occur due the human error, incorrect input, or the use of an incorrect application or tool. Natural disasters and calamities can also create issues. Databases must have policies and procedures to protect them from threats. The risk of unauthorized access increasing because of internet and intranets. The main motto of database security is to protect databases from losing data. Database security also allows or refuses for acting on the database. Admin can give privileges to a user.

1.1. Excess Privilege

When a user or an employee is given more privileges that can allow him to access or perform a task that is not expected from him then it can be harmful. An example of the company can be taken in which the administrator has access to the database and has privileges to change the records of employees. This may lead to a change in the personal or official information of any employee.

1.2. SQL Injection

Random SQL queries are fired by the attacker on the server. In the SQL statement, a string is given as an input. This is validated by the server. If it doesn't get validated it may get executed. Through this, an attacker may get the access to the database. He can alter, delete, or can leak the private data of an individual or a company. An example of an e-commerce website can be taken - if an attacker gets access to the database of an e-commerce website, he can change address or can get the card details.

1.3. Human Error

Human error is also a common threat that occurs many times. History has recorded that 90% of data breaches in 2019 occurred because of human error.

Factors causing human error are opportunity, environment and lack of awareness. Human error occurs when there is a chance or an opportunity. The environment is also a great example because if working environment is not good there are more often chances of a mistakes.

Human error includes many categories:

1.1.1. Weak Password

Passwords are the most basic to provide security, and they should not be shared with others. Simple passwords are very easy to crack. And the passwords which are shared among employees can also be dangerous.

1.1.2. Careless Handling of Data

Usually there are many positions in companies where employees work with a huge amount of sensitive data. These employees leak the data due to their carelessness, which may impact the company badly.

1.1.3. Buffer Overflow Attack

Buffer is the storage where the data is stored temporarily; when it is being transferred to a different location. A buffer overflow occurs when the data volume exceeds the buffer's storage capacity. An example of a login page can be taken. If a login page is designed for input of 10 bytes and if a user inputs 12 bytes then an error should be shown to the user to input only specific number of characters instead of accepting the user's input.

Attackers manipulate the buffer overflow problem by overwriting the memory. This change in the path of execution leads to damaging the file or exposing private information. An attacker can send new instructions to the application and gain access to it. If the attacker knows the memory layout of the page or application, he can deliberately give an input that a buffer cannot store.

1.4. Denial of Service Attack (DoS)

It is an attack where a legitimate user cannot access the service. There are many techniques by which an attack can be made. An attacker may get access and manipulate the server or resources. Overloading and network flooding are some of the techniques. DoS attacks can be serious threats to a company or organization.

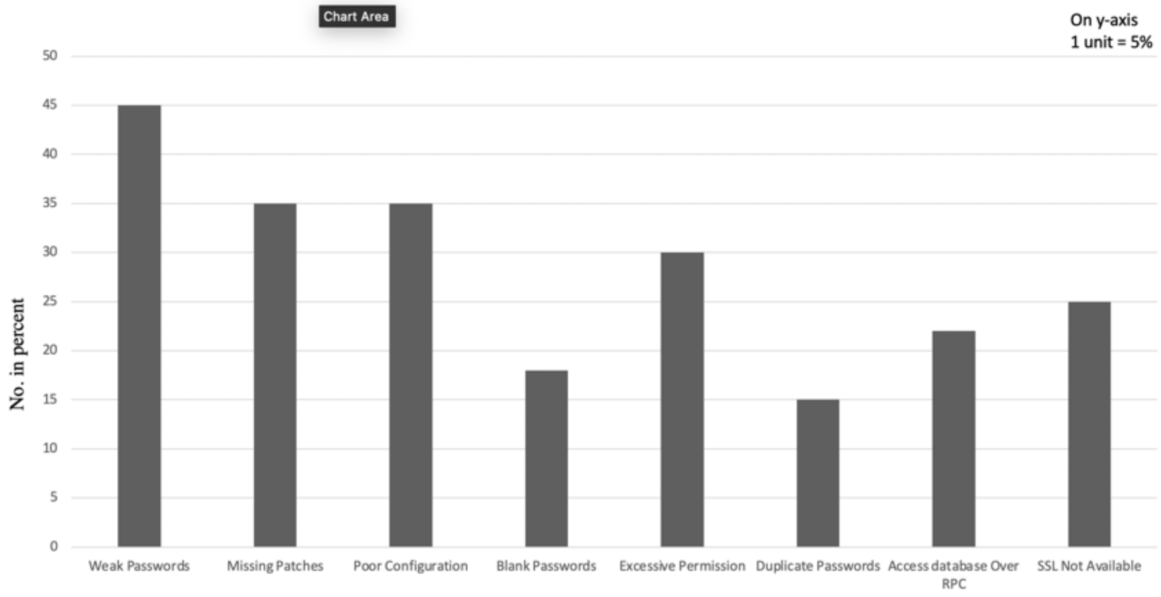
1.5. Malware

Malware is software that can take advantage of the openness, and can cause harm to a database. Malware can come through the endpoint connected to the network. So it is important to have protection from malware because the database may have some confidential information.

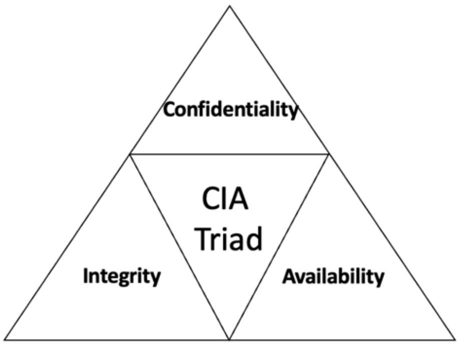
1.6. Unmanaged Sensitive Data

Nowadays, many companies are struggling to maintain databases with critical data. The database can have sensitive data; when it is lost or is insecure then it can cause problems. So it is very important to manage data to avoid the attacker to gain access to it.

3. Data Security Model



Common Database Security Issues



Data Security Model

CIA Triad is an important data security model which consists of 3 important security principles: confidentiality, integrity and availability. It is used by companies/organizations to implement proper security and control them, i.e. identify problems and resolve them.

Confidentiality says the data must be safe or private from an intruder or unauthorized access. Integrity says the data must be maintained properly throughout the process, and availability says the data must be available and easily accessible to an authorized user.

3.1. The Three Principles of CIA Triad

3.1.1. Confidentiality

This principle says that the data must be protected from unauthorized users to maintain confidentiality. To maintain confidentiality, we should keep proper authorization to access the database.

For example, an employee working for an organization/company in the administration department should have privileges to specific parts to maintain confidentiality.

If confidentiality is not maintained, important and secrete data may be leaked or in danger, and it can cause many problems such as blackmailing.

Confidentiality is maintained by implementing proper security i.e. 2FA (2 Factor Authentication), data encryption, and label restricted data.

3.1.2. Integrity

Integrity says data is not been tampered with and can be easily trusted. Integrity ensures protecting data that is stored or in transit; stored on a laptop or a portable device or in the cloud.

For example, withdrawal made from a bank account should reflect in the bank account database and be maintained properly.

If integrity is not maintained, data is worthless as it can corrupt and can harm the organization/company. Maintaining data includes data's accuracy, completeness and quality.

3.1.3. Availability

Availability refers to an authorized user having access to the resources when needed, for example when we enter a password on the laptop, we have access to all the files and folders (resources) in it, and we can perform any task on it.

If availability is not maintained the data, it is of no use; if an authorized user is not able to access the data on time, it is of no use; many consequences may occur. Data is not been updated due to not having access to the database.

We can improve availability in many ways. We can spread the data over the cluster so that the data is not lost. We can improve the load balancing aspect.

3.2. Importance of CIA in Security

Nowadays, a data breach has become a very recent problem for big organizations/companies. Data breaches are occurring due to poor security policies. CIA Triad is an important factor in security as it ensures data security. CIA Triad is also useful to address what went wrong.

4. Countermeasures against Threats

1. Create your own data centers or servers to prevent attacks.
2. Set up a proxy server to evaluate the request sent to the server.
3. The use of default networks must be avoided as attackers use default ports to brute force.
4. Use a real-time monitoring system to keep a watch on data breach.
5. Firewall should be used to secure the loopholes.
6. Data must be encrypted to keep sensitive information secrete.
7. Regular backups of database should be taken to prevent data loss because of any failure or attack.
8. Use of strong authentication is necessary as only passwords are not enough. Multi-factor authentication (MFA) should be used.
9. Access control must be implemented to prevent unauthorized access.
10. After database infrastructure is designed, it should be tested against attack to check its capabilities.
11. Password manager may be used to store passwords securely.
12. Disable network access when not in use so no attacker can access it.
13. We should limit the privileges to decrease the number of entry points.
14. Properly train the users.
15. Reduce the area of attack by not exposing ports, protocols and applications.
16. Use a programming language that lowers the chance of buffer overflow.
17. RAID must be used to prevent data loss due to disk failure.
18. Disable access through the public network so the user outside the organization cannot access it.
19. Udata should be cleared regularly so that unnecessary data do not make chaos.

5. Conclusion

Nowadays, databases face many security issues. Data is money in this era, so it must be secured and preserved properly. Many of the above mentioned threats are common in companies/organizations. Lost data may not be reclaimed sometimes, so security is a very important aspect. Physical damage is also a problem, like water damage, human error, fire, etc. We should look for strong security for less vulnerability. We can prevent these security threats by above mentioned techniques/countermeasures. Companies should give attention to loopholes and bugs. Companies should adopt some rules and regulations, and access control. For security, we should maintain the integrity, confidentiality and availability of the database.

References

1. A. Mousa, M. Karabatak, T. Mustafa, “Database Security Threats and Challenges”, 2020 8th International Symposium on Digital Forensics and Security (ISDFS), IEEE, June 2020. https://doi.org/10.1109/isdfs49300.2020.9116436
2. I. Basharat, F. Azam, A. Wahab Muzaffar, “Database Security and Encryption: A Survey Study”, International Journal of Computer Applications, Vol. 47, No. 12, pp. 28–34, 2012. https://doi.org/10.5120/7242-0218

3. B. Kumar, M. Hamed Said Al Hasani, “Database security — Risks and control methods”, 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), IEEE, pp. 334-340, 13-15 October 2016. https://doi.org/10.1109/cci.2016.7778937
4. K.M. Rajasekharaiah, Chhaya S. Dule, E. Sudarshan, “Cyber Security Challenges and its Emerging Trends on Latest Technologies”, International Conference on Recent Advancements in Engineering and Management (ICRAEM-2020), IOP Conference Series: Materials Science and Engineering, Vol. 981, 9-10 October 2020, 022062. https://doi.org/10.1088/1757-899X/981/2/022062