Database Security Threats and Challenges

Conference Paper · June 2020

DOI: 10.1109/ISDFS49300.2020.9116436

3 authors:

Abdulazeez Mousa
Nawroz University
5 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Murat Karabatak
Firat University
72 PUBLICATIONS **1,621** CITATIONS
SEE PROFILE

Twana Mustafa
Sulaimani Polytechnic University
9 PUBLICATIONS **134** CITATIONS
SEE PROFILE

Database Security Threats and Challenges

Abdulazeez Mousa
Department of Software Engineering
Firat university
Elazig, Turkey
abdulazizmoosa93@gmail.com

Murat Karabatak
Department of Software Engineering
Firat university
Elazig, Turkey
mkarabatak@firat.edu.tr

Twana Mustafa
Department of Software Engineering
Firat University
Elazig, Turkey
twanacsd@gmail.com

***Abstract*—with the growth and increasing sophistication of the Internet and the increasing dependence, it appeared more and more services over the Internet-based database, so it increases the risks facing databases. The number of attacks against these repositories has also increased. A database danger refers to an item, individual or other entity that poses a risk of misuse or manipulation of confidential data to an asset. Databases and computer properties are improperly secured in many business organizations. Databases should be protected rather than any system (device) in the enterprise. Most database security features have to be developed to secure the database environment. The aim of the paper is to underline the types of threats and challenges and their impact on sensitive data and to present different safety models. The assumption underpinning this study is that it understands the weaknesses, threats and challenges faced by databases, Database administrators will then work on developing a security strategy to help secure their databases.**

Keywords—Database security, security threats, attacks, security challenges, SQL injections.

I. INTRODUCTION

The great technological advancement, the development of various means of communication and communication, the openness of the world to some of it, and its dependence on sending various types of data through networks, This information is categorized into several types, most notably: Development Information: It is also called Development Information. This type includes information obtained from reading and reading books and articles, through which a person can acquire a number of modern terms and facts that aim to raise the scientific level of the human being. And expand his circle of cognition [7]. Achievement Information: It is the product of what the individual gets from new terms and concepts that motivate him to complete his work and accomplish it to the fullest, and thus make the right decision. Educational information: This is what the student acquires while he is in the study seats throughout the entire period of his education in all its stages, and the source of which is the curricula. Intellectual information: A set of assumptions and theories related to some kind of relationship that can be found between the dimensions of a problem. Research information: This is information that depends on conducting research and experiments and arriving at its results to access the necessary information, and it may be from scientific or literary. Systematic stylistic information: This type includes all information related to scientific methods that allow the researcher the opportunity to perform the research very accurately. Incentive information. Political information. Guidance information. Philosophical information. all of this has created a risk for the leakage of this data, and its access to wrong people or competitors, and thus has become an urgent need to maintain information security [8]. Information security is the complete control of information, in terms of determining who will receive this data, determining the powers to access it, and using a set of technologies to ensure that it is not penetrated by any party, and its importance multiplies from maintaining privacy, to preserving important data such as customer accounts in banks. The Internet has a habit of a wide range of vulnerabilities that enable unauthorized people to access this data, including programmatic errors that programmers make while building networks, or designing different applications, such as errors in how the application deals with the wrong entry, or because of bad Memory distribution, as there are many programmers who design programs to penetrate the systems, and look for their weaknesses. Resorting to a range of protection methods to maintain information security, including [9].

- Physical protection methods: There are many simple methods that must be followed in order to maintain the security of information, which is to keep the computer in a safe place, And to put a password on it to prevent tampering with intruders, and that the password contains letters, numbers, and symbols; Predict them, change them periodically.
- Firewall Use: A firewall is a device or application that is placed on the server and at network filters, each according to its needs.
- Encryption: There are many protocols designed to encrypt data, so that it prevents anyone who receives it from understanding it, and the degree of complications varies in this encryption. Encryption, and of course the decryption key is owned by the receiving device for this data.
- Data monitoring (Packet Sniffers): There are many applications that are able to know the movement of data coming out, and entering the network, and by analyzing it, it is possible to reach the breaches that occurred to this network, and know its location.

The greater the importance of data and its confidentiality, the greater the means used to protect it, from material and software, for example, server devices are placed in a place protected in various physical ways, including guards [9, 10].

In this article, we clearly research the threads of the information structures and provide a review of the existing security threads of the network. We first described the various types of threads that have been known to date. We have looked at the various methods by which the security threads of the database could be implemented into the program and defined which strategies could be used to handle these methods. Section II presented a related works of the database security threats and challenges, and in the section III we presented security threats arise from one or a variety of the following outlets. In the section IV we presented the challenges of the database security. And the in the section V we presented the types of the threats that faced database security and mentioned the Countermeasures of that threats.

978-1-7281-6939-2/20/$31.00 ©2020 IEEE

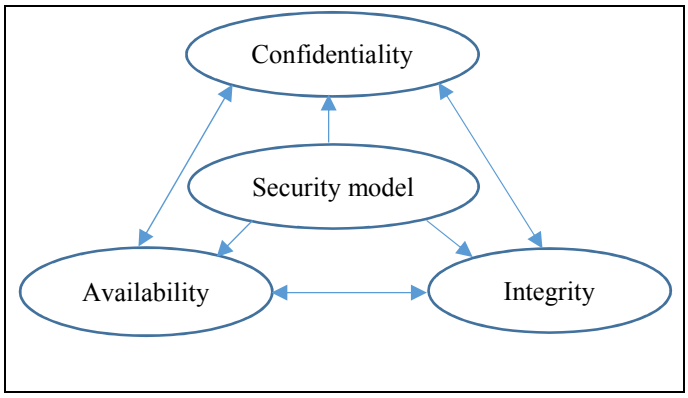

Fig. 1. CIA Triad

II. LITERATURE REVIEW

Saurabh Kulkarni1 and Siddhaling have written Review of Attacks on Databases and Database Security Techniques: in this paper Quite important and private information and there is a risk of an attack. This paper addresses multiple assaults on databases. Examination of several important database security strategies such as access management, SQLIA strategies, encryption and data scrambling are discussed. Any potential areas of study in the field of database security are often addressed in this article [1]. Sohail IMRAN and Dr. Irfan Hyder have written Security Issues in Databases: Security models, built for databases, vary in several ways because they concentrate on the various aspects of a database security issue or because they draw specific statements on what makes a stable database. Which leads to an imperfect and limited interpretation of the plan for organizational defense. This makes it impossible to balance the various health criteria. This paper addresses the various security problems in the databases. This strategy is useful for the preparation of transparent and tailored security specifications for databases. Safety concerns and specifications are addressed in this paper on optional and compulsory protection frameworks to secure conventional and focused database networks. We also address security-related problems in a realistic, database-oriented manner. A short review of past and current trends in the security of databases is given. And various security problems related to information systems and unbiased information systems. Many optional plans are given Mandatory security frameworks for defense Conventional databases and object-oriented database systems. However, there is still no requirement for the construction of such safety types. The research presented in this paper points out a variety of specific security database issues; it can be extended to identify, develop and enforce an efficient security strategy on a database that provides the world with a consistent description of the integrity of the database [2]. ILO Somtoochukwu F, Ubochi Chibueze and Osondu U. S have written Core Threats and Prevention in Database Security: Database safety is an increasing issue, as the number of recorded events increases due to lack of or unintended access to confidential data. When the number of data gathered, stored and exchanged electronically rises, so will the need to consider the reliability of the information. Database protection can provide secure and safe access to database information, in addition to ensuring data confidentiality, accuracy and overall efficiency. Database security, in effect, aims to ensure that only approved users execute authorized tasks at authorized times. This article focuses on computer protection principles and processes. Database security requires, in this case, three structures, secrecy or defense of data from unauthorized release, incorporation or avoidance of unauthorized access to data, And the detection or recognition of hardware and software failures or malicious operation or recovery that leads to a failure to make data accessible. Database protection involves sub-topics.

These issues include ransomware, weak security, inappropriate database setup, SQL injection, cross-request, and misuse of disproportionate rights (grant / revocation). This research has been concluded by reviewing data management techniques that can help us secure our machine knowledge [3]. Erez Shmueli, Ronen Vaisenberg, Yuval Elovici and Chanan Glezer have written Database Encryption – An Overview of Contemporary Challenges and Design Considerations: This article discusses the key problems and architecture issues relevant to the encryption of databases. The first article gives an overview of attack and significant problems related to computer protection, public encryption, key control and fingerprint incorporation. The paper discusses the recent theoretical research on alternate encoding solutions relative to the position of the encryption; encrypted data indexing; and key management. Finally, the article ends with a specification that follows the specific design criteria: encryption layout, encryption reliability, and key safety. In this study, we concentrate on theoretical research and suggest a design-oriented architecture that can be used by originally database security vendors and external stakeholders, as well as by DBAs and enterprise information technology developers. Based on our analysis, multiple configurations for the implementation of database encryption are compared. To sum up, the maximum performance is obtained when coding is performed within the DBMS. File device encryption, though easy to install, does not require the use of multiple encryption keys and does not enable the data collection to be encrypted / decrypted and thus has a significant effect on both data protection and efficiency. And summarizes the impact of coding precision on a variety of factors. Enhanced efficiency and management of the database structure cannot be accomplished with maximum page or table information precision.Nevertheless, different methods can be used to deal with unwanted changes and leakage of information by using individual values or encoded record / node precision [4]. Shivnandan Singh and Rakesh Kumar Rai have written A Review Report on Security Threats on Database: Data is one of the most critical things for any company. As we know, the database is a set of data and programs for carrying out computer operations. So for any enterprise we have to protect our data for a good ride. So in this article, we need to concentrate on database-based threats as well as some algorithms based to database security. Databases have the highest rate of infringements of all company properties, According to the 2012 analysis of Verizon Data breaches. Verizon revealed that 96 percent of the documents accessed were from libraries, and the Free Technology Foundation estimated that 242.6 million documents had potentially been hacked in 2012. The repositories are the foundation of many apps today. They are the primary source of storage for a variety of organizations. As a result, attacks on databases are also growing, because they are a very dangerous type of attack. They can disclose main or significant details to the intruder. This paper addresses multiple assaults on databases. Analysis of several important database security strategies such

as access management, SQLIA strategies, encryption and data scrambling are discussed. Any potential areas of study in the field of database protection are also discussed in this article. This work will contribute to a more practical approach to the problem of database stability [5]. Nedhal A. Al-Sayid and Dana Aldlaeen have written Database Security Threats: A Survey Study: The databases are the archives of the most important and important knowledge within the organization. With increased access to data contained in databases, attacks on these databases have grown in frequency. A database threat refers to an item, person or other individual that is at risk of missing or damaging source-sensitive data. Today, in other industry organizations, Databases and properties are poorly secured. Databases must be protected rather than any device in the enterprise. A variety of database protection models are expected to be built to protect the database environment. The aim of the article is to show the kinds of threats and their impact on sensitive information, And to offer a range of security models. The premise behind this analysis is that by recognizing the flaws and risks posed by databases, database managers will begin to develop a security plan to help protect their databases. Data confidentiality is a central component of many operating systems. In this article, we addressed a questionnaire and a summary of the existing protection threads in the database. We first described the various forms of strands that have been known to date. They have looked at the various methods by which the authentication chains of the database can be extended and established techniques that have been able to deal with the methods. When combating database risks, organizations need to recognize the security of databases as part of their overall security policy. Risks can be greatly minimized by concentrating on the more serious risks. Both information properties (for individuals, systems and technologies) are subject to the introduction of avoidance, monitoring and correction measures. They need to work intensively to decrease vulnerabilities and evolve newer technologies to detect and prevent security threats. This would help to protect the safety and confidentiality of sensitive data and improve operating productivity across diverse and heterogeneous environments [6].

III. Security Threats Arise From One Or a Variety of The Following Outlets

- External threats: -External attacks come from outlets outside the organization. Examples cover hackers, organized crime gangs and policy agencies, as well as environmental disasters. Usually, no trust or right is inferred for external institutions.
- Internal threats: -The origins of internal attacks emerge from inside the company. That includes human assets — company managers, staff and interns. Most insiders are trusted to a degree and others; IT managers, in general, have a higher level of control and privilege.
- Partner: -Partners include every third party who has a contractual partnership with the company. This supply chain of associates, manufacturers, manufacturers, vendors and consumers is known as the expanded business. The sharing of information is important for the expanded company and, for this reason, a certain amount of trust and privilege is typically assumed between all the business partners and not as an independent document. Please do not revise any of the current designations.

IV. Database Security Challenges

The database can be viewed at three various levels of abstraction. Usually, a three-level perspective is introduced, including an internal dimension, representing the physical storage of the database and the physical processing of the data, A logical (or conceptual level) level that provides users with a high level explanation of the physical world that the database represents; and an objective level (or view level) that defines the views that various users or programs have on the storage data. Just section of the entire database is defined at this point. The internal dimension maps the abstract structures provided by the data model to the actual structures in the underlying operating system. In addition to access and processing facilities, each DBMS must also have security measures to ensure confidentiality, honesty and accessibility of data stored[7, 12].

This is a common practice for organizations to protect the enterprise at the level of the network, as a rational approach because all risks are external. However, according to CERT's annual report, up to 50% of the network attacks come from inside. In fact, that's why many organizations are implementing a second protection level made up of point-of-the-art technologies that secure databases. In the case of data privacy against security attacks, the quality of the data is perceived to be an indicator of the value given to the data by its user. There are several reasons to identify data responsiveness [12].

- The meaning of a data itself can be so exposing or secret that it is vulnerable.
- The origins of a data might suggest the need for confidentiality.
- The specific trait or record could have been considered to be vulnerable.
- Any data will not be vulnerable on its own, but may become vulnerable in the presence of any other data.

The details and the general cyber management issues are the main aspects of technology that have a significant effect on businesses today. Server protection can be exposed to danger by accessing confidential data, modifying data, etc. Degrading the functionality of the website or doing serious harm to the credibility of the client and industry. Each IT system must be categorized according to the most important data collected, interpreted or distributed by the IT system[9, 11].

V. Threats And Countermeasures of Databases Security

Data is a very important commodity for every organization. Every day, businesses globally gather a lot of details on their day-to-day activities and clients. Data is stored in libraries that are used to manage data and to automate different processes inside and outside organizations. Because of its absolute value, Data security is a core component of data safety. Data storage is the objective of every database management system (DBMS), also known as database stability. However, that's not always the case. In this post, we can hear more about database security risks and what the management departments and company owners can do to secure the database.

Database security starts with physical security. That is why only approved workers should have access to the physical database.

However, there are also other internal and external risks to databases, some of which are mentioned below.

- SQL Injections. This is a form of attack where the malicious code is inserted in the frontend (web) applications and transferred to the backend database. As a result of SQL injections, computer attackers have unrestricted access to all data contained in a database. There can be two kinds of such code attacks: SQL injection targeting standard databases and NoSQL injections targeting massive databases.

  Countermeasures:

  - The processed protocol is used instead of direct queries.
  - MVC Architecture is to be applied.

- DB Vulnerabilities and Misconfigurations. It also occurs when databases are discovered to be absolutely inaccessible due to mis-configuration. In addition, some databases have default accounts and configuration parameters. This should be noted that hackers are also highly skilled This professionals who certainly know how to manipulate database vulnerabilities and mis-configurations and using them to target the business.

  Countermeasures:

  - The systems are not expected to have any default accounts.
  - The IT workers will be highly trained and experienced.

- Denial of service attack. This form of attack slows down the database server and could also make it inaccessible to all users. Despite the fact that the DoS attack will not expose the contents of the database, it will cost the victims a lot of time and resources. What's more, what's the point of a website if you can't use it or navigate it [12].

  Countermeasures:

  - TCP / IP stack is reinforced by adding the correct registry settings to maximize the size of the TCP connection list.
  - Decrease the time of creation of the relation.
  - Using dynamic backlog structures to guarantee that the queue of the link is never exhausted.
  - Using the Intrusion Detection System (IDS) network.

- Unmanaged Sensitive Data. Often businesses hold a lot of confidential information and do not maintain an complete inventory of it. Forgotten and unattended data can be a victim of hackers. In fact, new critical data were introduced on a regular basis so it is not easy to keep track of all this. This means the recently inserted data can be vulnerable to risks [7,11].

  Countermeasures:

  - Encrypt all of the confidential data in the database(s).
  - Apply the necessary controls and permissions to your servers.
  - Run a regular scan for new important data in the repositories. You can do that very easily with the Regular Data Discovery platform and the Enforcement Manager, which can immediately discover and secure newly introduced confidential data.

- Database Backups Exposure. It's a good idea to backup proprietary repositories at specified time frames. However, oddly, database backup files are also left totally unprotected from attack. As a result, frequent security vulnerabilities arise by database backup leaks.

  Countermeasures:

  - Encrypt the files and copies. Storing data in encrypted form helps all output and backup versions of databases to be secured. Data Sunrise Data Encryption is the only way to do so.
  - Auditing all the servers and copies. Using so helps you see who's been trying to get access to confidential info.

- Excessive Database Privileges: Users of the database can have different rights. Users can, however, misuse them, and here are the major forms of privilege misuse: unnecessary privilege abuse, permissible privilege abuse, and unused privilege abuse. Excessive rights often lead to needless dangers. According to estimates, 80 per cent of assaults on company websites are carried out by existing client workers or ex-employees[5].

  Countermeasures:

  - It is recommended that a stringent access and privilege management policy be enforced and maintained.
  - Don't give client staff excessive rights and revoke expired rights in time.

- Malware: Malware will infiltrate different computers and cause legitimate users to allow data to be accessed because the malicious code installed in their computer exploits their access capability to enter the enterprise.

VI. Conclusion

Data confidentiality is a central component of many operating systems. In this article, we discussed a questionnaire and a review of security risks to the existing database. We first described the various forms of strands that have been known to date. We have looked at the various methods by which the authentication chains of the database can be extended and established techniques that have been able to deal with the methods. When combating database risks, organizations need to recognize the security of data bases as part of their routine security policy. Risks can be greatly minimized by concentrating on the more serious risks. Both information properties (for individuals, systems and technologies) are subject to the introduction of avoidance, monitoring and correction measures. They need to take a job intensively to develop a bugs and incorporate emerging technology to track and deter security threats. This would help to protect the safety and confidentiality of sensitive data and improve

operating productivity across diverse and nonhomogeneous environments. Future work will be more details to enhancing security by reducing threats and risks field of Database Security.

REFERENCES

[1] S. Kulkarni, S. Urolagin, “Review of Attacks on Databases and Database Security Techniques”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 2, Issue 11, November 2012.

[2] S. Imran and I. Hyder, "Security Issues in Databases," 2009 Second International Conference on Future Information Technology and Management Engineering, Sanya, 2009, pp. 541-545, doi: 10.1109/FITME.2009.140.

[3]V. Pevnev and S. Kapchynskyi, "core threats and prevention in database security", Advanced Information Systems, vol. 2, no. 1, pp. 69-72, 2018. Available: 10.20998/2522-9052.2018.1.13.

[4] E. Shmueli, R. Vaisenberg, Y. Elovici and C. Glezer "Database Encryption – An Overview of Contemporary Challenges and Design Considerations" ACM SIGMOD Record pp. 29-34, 2010

[5] S. Singh, and R. Rai. "A Review Report on Security Threats on Database." International Journal of Computer Science and Information Technologies Vol. 5, pp. 3215-3219, 2014.

[6] N. A. Al-Sayid and D. Aldlaeen, "Database security threats: A survey study," 2013 5th International Conference on Computer Science and Information Technology, Amman, pp. 60-64, 2013.

[7] M. Murray, Coffin, "Database Security: What Students Need to Know." Journal of Information Technology Education, vol. 9, pp 61-77, 2010.

[8] R. Agrawal, R. Srikant, and Y. Xu. "Database technologies for electronic commerce." Proceedings of the 28th International Conference on Very Large Databases. Morgan Kaufmann, vol .2, pp.1055-1058, January 2002.

[9] A. Furmanyuk, M. Karpinskyy and B. Borowik, "Modern Approaches to the Database Protection," 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, pp. 590-593, September 2007.

[10] A. Asmawi, Z. M. Sidek, and S. A. Razak , “System Architecture for SQL Injection and Insider Misuse Detection System for DBMS”, In 2008 International Symposium on Information Technology, vol. 4, pp. 1-6, June 2008

[11] P. B. Ambhore, B. B. Meshram, and V. B. Waghmare, "A Implementation of Object Oriented Database Security," 5th ACIS International Conference on Software Engineering Research, Management & Applications (SERA 2007), Busan,vol. 7, pp. 359-365, , 2007.

[12] Ş. Mariuţa, "Principles of security and integrity of databases." Procedia Economics and Finance, Targul din Vale, Romania, vol. 15, pp. 401-405, October 2014.

[13] M. Karabatak and T. Mustafa, "Performance comparison of classifiers on reduced phishing website dataset," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, vol. 5, pp. 1-5, 2018.