

Shilkov Danil Anatolyevich

Student

Ural Federal University named after the first

President of Russia B.N. Yeltsin

Russia, Ekaterinburg

Academic supervisor: Kovaleva Alexandra Georgievna

MAIN ASPECTS OF DBMS SECURITY

***Abstract.** The paper is devoted to database security - the prohibition of unnecessary disclosure of information and modification of data while ensuring the availability of necessary services. A number of security methods have been created to protect databases. Many security models have been developed based on various aspects of database security. All of these security techniques are useful only when the database management system is designed and developed to protect the database. Recently, the growth of a web application with a database in its Secure Database Management System backend is more important than just a secure database.*

***Keywords:** vulnerability, threats, security methods, DBMS.*

Шильков Данил Анатольевич

Студент

Уральский федеральный университет имени первого

Президента России Б. Н. Ельцина

Россия, г. Екатеринбург

Научный руководитель: Ковалева Александра Георгиевна

ОСНОВНЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ СУБД

***Аннотация.** Статья посвящена безопасности баз данных - запрету ненужному раскрытию информации и модификации данных при обеспечении доступности необходимых услуг. Для защиты баз данных был создан ряд методов безопасности. Многие модели безопасности были разработаны на основе различных аспектов безопасности базы данных. Все эти методы защиты полезны только тогда, когда система управления базами данных разработана и развивается для защиты базы данных. В последнее время рост веб-приложения с базой данных в бэкэнде Secure Database Management System является более важным, чем просто защищенная база данных.*

***Ключевые слова:** Уязвимости, угрозы, методы защиты, СУБД.*

Database management systems, especially relational databases, have become the dominant tool for storing large amounts of information. Any developed information applications rely not on file structures of operating systems, but on multi-user DBMSs executed in client/server technology. In this regard, ensuring the information security of DBMS, and especially their server components, is crucial for the security of the organization.

For DBMS, all three main aspects of information security are important: confidentiality, integrity, and availability. The General idea of database protection is to follow the recommendations formulated for security class C2 in the «criteria for evaluating reliable computer systems» 0. Some DBMSs offer extensions specific to class B1, but the practical application of such extensions makes sense only if all components of the organization's information structure meet the security category B. This is not easy to achieve, both from a technical and financial point of view. There are also two things to consider. Firstly, for most commercial organizations, the C2 security class is enough. Secondly, the more secure versions lag the usual in terms of content capabilities, so the advocates of secrecy, in fact, are doomed to use outdated (although carefully tested) products with all the ensuing consequences in terms of maintenance.

Almost all major DBMS manufacturers are limited to developing the concept of confidentiality, integrity, and availability of data, and their actions are mainly aimed at overcoming existing and already known vulnerabilities, implementing basic access models, and addressing issues specific to a DBMS. This approach provides solutions to specific problems but does not contribute to the emergence of a General security concept for such a class of SOFTWARE as a DBMS. This significantly complicates the task of ensuring the security of data warehouses in the enterprise.

The importance and value of enterprise information leads to the need of protecting not only the infrastructure elements, but also the databases themselves. The purpose of the research is to comprehensively review and systematize the security issues of various database management systems (DBMS) in accordance with new threats, General trends in the development of information security and their increasing role and diversity 0.

There are many ways of securing the database. These ways are based on different aspects of securing the database. As mentioned in the introduction a complete solution to data security is fulfilled according to the following three requirements: Confidentiality, Integrity, Availability (CIA).

Means to the protection of data against unauthorized disclosure can be achieved using access control mechanism. The encryption technique is applied to data stored on secondary storage or transmitted on a Network.

Means to the prevention of unauthorized and improper data modification can be achieved in combination of access control mechanism by semantic integrity constraints.

Means to the prevention and recovery from hardware and software errors and from malicious data access denials making the database system inaccessible. The data that are available on the Web can be powered by the use of techniques protecting against denial-of-service attacks and attacks based on machine learning techniques 0.

Modern DBMSs support both selective and mandatory approaches to data security. In the case of selective management, a certain user has different rights, or

privileges, and permissions when working with different objects. Since different users may have different access rights to the same object, such systems are very flexible. In the case of mandatory management, each object is assigned a certain qualification level, and each user is granted access rights to a particular level; and accordingly, if you have access rights to a certain level-everything that is recorded at this level, you have access to everything. It is believed that such systems are rigid, static, but they are easier to manage and the user then can assign access to up to 5th to 6th to 7th level, etc. in increasing order of priority 0.

In normal DBMSs, either the appropriate operating system mechanism is used to identify and authenticate the user, or what is available in the connection with SQL statement (there are special parameters for connection access). When starting a session with the database server, the user identifies the contact, or login, with their name, and the password serves as the authentication tool.

An ID is a short name that uniquely identifies the user for the DBMS. It is the basis of security systems. Appropriate accounts are created for users. Identification allows the subject (i.e., the user or process acting on behalf of the user) to identify itself, i.e. to provide its name (login). By means of authentication (i.e. authentication), the second party (the operating system or the DBMS itself) is convinced that the subject is really who he claims to be. Authorization refers to a service that guarantees that the user is allowed access to a resource. This service determines whether the authenticated client has the right to use an object.

For particularly vulnerable systems (for example, banking systems, etc.), more complex security systems are used. For example, there are known systems with the sequential creation of several personal questions, with a limited time to answer them and the number of attempts (as in any mobile phone).

The ANSI ISO standard uses the term «authorization ID» instead of the term «user ID».

The security system on the server can be organized in 3 ways:

1. standard security: when separate access is required to the server (i.e. you log in to the operating system with one password, and to the database server with another);

2. integrated security (quite often used): log in to the operating system with a user password, and the same name with the same password is registered in the DBMS. You don't need to log in a second time. Once a person got on the server, well, okay, let them use everything they have.

3. a mixed system that allows you to enter both the first and second way.

The DBMS uses arbitrary access control is obtained when the owner of an object (in extreme cases, the database administrator, but more often the owner) transfers access rights (permissions) to someone. However, rights can be assigned to individual users, groups of users, or roles.

The main source of threats that are specific to a DBMS is a database. The main tool for interacting with a DBMS is the SQL language, which is a powerful non-procedural tool for defining and manipulating data 0. Stored procedures add control constructs to this repertoire. The rules mechanism makes it possible to build complex, difficult to analyze chains of actions, allowing implicitly transfer the right to perform procedures, even without having, strictly speaking, the authority to do so. As a result, a potential attacker gets their hands on a powerful and convenient tool, and the development of the DBMS is aimed at making this tool even more powerful and convenient.

There are several threats that occur when an attacker uses SQL tools. Aggregation is a method of obtaining new information by combining data obtained legally from various tables. Aggregated information may be more secret than any of the components that compiled it. As an example, you can consider a database that stores the parameters of all the components that will be used to assemble the rocket, and Assembly instructions. Data on each type of component is required by suppliers, Assembly instructions (insert part A in hole B) - Assembly production [1].

Information about individual parts is not secret in itself. At the same time, the analysis of the entire database allows finding out how to make a rocket, which can be considered as a state secret. Increasing the level of data secrecy during aggregation is quite natural - it is a consequence of the law of the transition from quantity to quality. The aggregation is fought by carefully designing the data model and limiting user access to information as much as possible.

If a user has access to all the features of SQL, they can easily make it difficult for other users to work (for example, by initiating a long transaction that captures a large number of tables). Modern multithreaded DBMS servers reflect only the most straightforward attacks, which consist, for example, in launching mass data loading operations during «peak hours». It is strongly recommended not to give users direct SQL access to the database by using application servers as filters.

Database management systems (DBMS), especially relational DBMS and expert systems (ES), have become the dominant tool in data storage, processing, and presentation. Any failure in the operation of the DBMS (ES), accompanied by the loss, albeit temporary, of access to data, immediately affects the competitive ability of the enterprise. Therefore, the protection of data from unauthorized access, from unauthorized modification or simply from their destruction is one of the priority tasks in the design of any information system. This problem (the problem of data protection) is connected both with physical protection of data and system programs, as well as with the protection against unauthorized access to data transmitted over communication lines and stored on storage devices, resulting from the activities of both unauthorized users and special virus programs 0.

REFERENCES

1. Krunoslav Arbanas, Nikolina Žajdela Hrustek. Key Success Factors of Information Systems Security. – December 2019. – URL:

https://www.researchgate.net/publication/338249493_Key_Success_Factors_of_Information_Systems_Security.

2. Neerja Bhatnagar. Security in Relational databases - In: Handbook of Information and Communication Security. ed. by P. Stavroulakis, M. Stamp. - Springer. - January 2010. - pp. 257-272 - URL: https://link.springer.com/chapter/10.1007/978-3-642-04117-4_14.

3. Polk T. W., Bassham L. E. Security Issues in the Database Language SQL. - NIST Special Publication 800-8. - August 2, 1993. - URL: <https://csrc.nist.gov/publications/detail/sp/800-8/archive/1993-08-02>.

4. Pradeep K. Murukannaiah, Chinmaya Dabral, Karthik Sheshadri. Learning a Privacy Incidents Database. - April 2017. - URL: https://www.researchgate.net/publication/314288016_Learning_a_Privacy_Incidents_Database.

5. Skakun V. V. Protection of information in databases and expert systems. - Minsk, 2017. - pp. 6-115. - URL: <https://elib.bsu.by/bitstream/123456789/48524/5/Защита%20информации%20в%20БД.pdf>.