Methods of Modeling Database System Security

Svitlana Rzaieva[1], Dmytro Rzaiev[2], Yuliya Kostyuk[1], Hennadii Hulak[3], and Oleksandr Shcheblanin[4]

[1] *State University Of Trade And Economics of Kyiv, 19 Kyoto str., Kyiv, 02156, Ukraine*
[2] *Kyiv National Economic University of Kyiv, 54/1 Beresteysky prospect, Kyiv, 030 Ukraine*
[3] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[4] *University Passau, 41 Innstraße, Passau, 94032, Germany*

Abstract

Ensuring the protection of information stored in databases from unauthorized access, loss, and damages, as well as ensuring the confidentiality, integrity, and availability of data is a fundamental task of database security. The article explores the identification of potential threats and their analysis, the determination of possible consequences, and the development of protection strategies to prevent these threats. The identification of threats is closely linked to the process of threat modeling to enhance the security of databases. The article explores various threat modeling methods, such as threat analysis, scenario modeling, mathematical modeling, vulnerability analysis, risk analysis, and others. Each of these methods helps determine which threats may impact the database system and what security measures can be taken to prevent them. The article also describes a security model for a database system, including data vulnerability analysis, attack modeling, analysis of data from previous attacks, access rights analysis, determination of protective measures, and security method testing. This model serves as a tool for effectively managing risks and ensuring information security in today's world, where cyber threats are becoming increasingly serious and widespread.

Keywords

Database security, potential threat identification, threat modeling, vulnerability analysis.

1. Introduction

Methods for modeling the security of database systems are recognized as extremely important in the modern digital world, where information has become one of the most valuable assets for many organizations and institutions. The increasing volume and significance of data for business and scientific research make databases a target for various cyber threats. Attackers actively seek to gain access to this valuable information, making data protection a serious daily task for every organization. The rapid development of technologies such as cloud computing and the Internet of Things (IoT) expands the range of attacks on database systems and creates new opportunities for malicious actors, emphasizing the importance of developing effective security modeling methods [1–3].

High public and regulatory attention to data privacy protection, such as the General Data Protection Regulation (GDPR) in the EU, imposes significant requirements on companies and organizations regarding the protection of personal data. This necessitates project developers to design and implement effective modeling and risk management methods to ensure compliance with relevant legislation [4, 5].

The increasing level of professionalism among cybercriminals and the complexity of attacks underscore the need for continuous improvement of security measures [6]. The relevance of the article lies in the development and enhancement of threat modeling methods

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: rzaevasl@knute.edu.ua (S. Rzaieva); rzaiev@kneu.edu.ua (D. Rzaiev); kostyuk_yu@knute.edu.ua (Y. Kostyuk); h.hulak@kubg.edu.ua (H. Hulak); oleksandr.shcheblanin@gmail.com (O. Shcheblanin)
ORCID: 0000-0002-7589-2045 (S. Rzaieva); 0000-0002-7149-4971 (D. Rzaiev); 0000-0001-5423-0985 (Y. Kostyuk); 0000-0001-9131-9233 (H. Hulak); 0009-0001-0614-6540 (O. Shcheblanin)

for the timely detection and prevention of attacks on database systems [7, 8].

2. Previous Research

In [9], various threats faced by almost all software systems are discussed as technologies evolve. These threats can originate from external or internal sources, and their impact can be devastating. Systems may cease to function entirely, or there may be a leakage of confidential information, affecting consumer trust in the system provider. To prevent the exploitation of system vulnerabilities by threats, the authors suggest using threat modeling methods to think defensively.

[10] addresses security issues in enterprise systems based on the MITRE Enterprise ATT&CK matrix. This matrix focuses on describing system assets, attack steps, defense mechanisms, and asset associations. The entity-relationship model describes enterprise IT systems as a whole, using available tools, allowing the simulation of attacks on instances of the system model. These simulations can be used to investigate security configurations and architectural changes for more effective system protection.

[11] explores traditional approaches to threat modeling, such as Microsoft's STRIDE, where Data Flow Diagrams (DFD) are used as the primary input material for threat analysis.

[12] discusses various threats and vulnerabilities that may arise in the development, management, and maintenance of different databases and database management systems. The article aims to analyze the described threats and provide the most appropriate solutions for database security.

3. Issues

Database system security includes a wide range of issues and aspects aimed at protecting data stored in the database from unauthorized access, loss, damage, confidentiality, integrity, and availability of data. Database security includes the identification of potential threats and the development of protection measures to prevent these threats.

Identification of potential threats is the process of identifying and analyzing various possible threats, both external and internal, that is, dangerous events or situations that may occur and lead to loss, damage, or unauthorized access to information stored in the database. These threats can include various aspects, such as technical attacks from intruders, software bugs, improper security settings, natural disasters, or internal threats from employees. To effectively manage these potential risks, it is necessary to identify them, understand their possible consequences, and develop protection strategies.

Identifying potential threats is closely related to the process of threat modeling to improve database security. The first step in this process is to identify the various possible threats that may arise in the context of the database. This includes analyzing external and internal factors that can create potential risks to information security. This analysis may include assessing potential attacks, identifying system vulnerabilities, and assessing the possible consequences of possible threats to the confidentiality, integrity, and availability of data.

Once identified, threats can be used to create a threat model that describes their nature, potential attack vectors, and risk assessment. The threat model can then be used to develop protection strategies, prioritize security measures, and establish access control rules to help prevent or mitigate potential threats. Thus, identifying potential threats and modeling them are key steps in implementing effective database security measures.

Threat modeling methods are approaches and techniques used to analyze identified threats and risks in the areas of security, information security, cybersecurity, and other fields. These methods help to assess what threats may affect an organization, system, or project, and what measures can be taken to prevent or mitigate those threats. Here are some basic threat modeling techniques.

The threat analysis method includes the identification of existing threats, their characteristics, and the ability to affect the system or organization. Standard SWOT analysis (analysis of strengths, weaknesses, opportunities, and threats) and other approaches to identify threats.

The scenario modeling method provides the creation of various scenarios based on known threats and their impact. Scenarios help to prepare action plans for different possible conditions.

Mathematical modeling is used to analyze threats and their impact on systems, including modeling probable threat cases, identifying risks, and calculating possible losses.

Vulnerability analysis method—assesses existing vulnerable systems or organizations that can be exploited by attackers to implement a threat. After identifying vulnerabilities, protection strategies are developed.

The risk analysis method involves assessing the likelihood of threats and the impact of these threats on a system or organization. As a result of risk analysis, specific risks and their level of danger can be identified.

The attack modeling method provides a simulation-type attack model. Simulation confirms what methods can be used by attackers to interfere with the system and how it can affect its operation.

Creating a risk matrix, developed to systematize and compare different risks based on their probabilistic nature and impact on the system. This allows the authorized person to make decisions about the prioritization of risk management.

The protection cost analysis method estimates the costs that may be associated with preventing or remediating the consequences of threats. By taking into account the costs, the authorized person can make informed decisions about investing in security controls.

Business impact analysis method—this method assesses the possible consequences of a threat and its impact on the organization's operations. Taking this impact into account, the organization can develop strategies to ensure business continuity.

Monitoring and updating. Threat and risk models need to be constantly updated, after which new threats are reflected, and known threats can change the existing characteristics. It is also important to monitor and evaluate the effectiveness of protection measures to ensure that they are effective.

Threat modeling techniques are an important part of a risk management and security strategy in today's world, where cyber threats and other forms of threats are becoming increasingly complex and widespread.

Database security modeling is an essential aspect of ensuring the security of information and data. It helps identify external and internal threats to the database system and develop strategies for their protection. For a better understanding of the methods of modeling database security, the authors used the tools of the Mind Map programming platform to construct a corresponding model. This model consists of the following key modeling methods:

1. Data vulnerability analysis.
2. Database attack modeling.
3. Analysis of data on previous attacks.
4. Database access rights analysis.
5. Determination of protective measures and the creation of a response plan to external and internal threats.
6. Security methods testing.

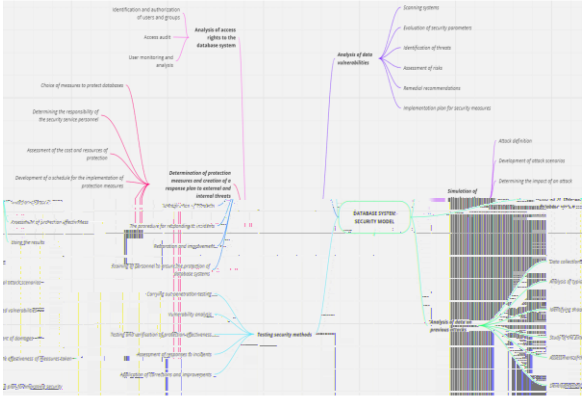
Identification and authorization of users and groups
Access audit
User monitoring and analysis
Analysis of access rights to the database system
Choice of measures to protect databases
Determining the responsibility of the security service personnel
Assessment of the cost and resources of protection
Development of a schedule for the implementation of protection measures
Determination of protection measures and creation of a response plan to external and internal threats
Assessment of protection effectiveness
Using the results
The procedure for responding to incidents
Restoration and improvements
Training of personnel to ensure the protection of database systems
Carrying out penetration testing
Vulnerability analysis
Testing and verification of protection effectiveness
Assessment of responses to incidents
Application of corrections and improvements
Testing security methods
Analysis of data vulnerabilities
Scanning systems
Evaluation of security parameters
Identification of threats
Assessment of risks
Remedial recommendations
Implementation plan for security measures
Attack definition
Development of attack scenarios
Determining the impact of an attack
Simulation of
DATABASE SYSTEM SECURITY MODEL
Analysis of data on previous attacks
Data collection

Figure 1: The model of database security system modeling methods is built using the Mind Map software tool. Source: constructed by the authors themselves (screen capture)

Let's delve into each modeling method in the model of threats. Data Vulnerability Analysis involves addressing identified weaknesses in the isolation and protection of data in the database system. The first step in data vulnerability analysis is identifying potential vulnerabilities in the database system, such as software deficiencies, inadequate access rules, or insufficient password protection. This stage includes the following steps:

- Conducting a system scan to identify vulnerabilities in the database configuration and software.
- Evaluating security parameters, including access rights, password policies, table and view access permissions, file settings, and other database security parameters.
- Identifying potential threats that could be used to breach the database system, including external and internal attacks, as well as other threat scenarios.

- Assessing the impact of vulnerabilities on the database system and their likelihood, and identifying critical vulnerabilities requiring immediate resolution.
- Determining specific measures to address vulnerabilities, including patches, software updates, changes to access rights, and other measures.
- Developing a plan and setting priorities for implementing recommendations to ensure a phased improvement in data security.

Attack Modeling on a database system involves the process of defining and simulating potential attacks on the database system. In attack modeling, a model is created that generates the process of system intrusion, how attackers may attempt to breach the system, and the methods they may use. This process may include SQL injections, session hijacking, password attacks, exploiting software vulnerabilities, and more. This approach provides a deep understanding of potential threats and identifies weaknesses in the database system's security. Let's explore this process in more detail.

The first step in the attack modeling process is defining selected attacks, which means identifying various types of attacks that may be involved in malicious attempts to breach the database system. This may include external attacks such as SQL injections, session hijacking, and password attacks, as well as insider attacks involving malicious actions by employees or unauthorized users.

The next step in the attack modeling process is developing attack scenarios. Detailed scenarios must be created for each identified attack, describing how the attack may occur. This includes the sequence of actions needed for a successful attack, including SQL queries that may be used and other critical details.

Another crucial step is assessing the impact of the attack, meaning evaluating the impact of each attack on the database system, including aspects of data confidentiality, integrity, and availability.

Attack Simulation. At this stage, simulation tools and techniques are used to reproduce attack scenarios in a controlled environment. Specialized tools can be employed to execute SQL injections or session hijacking to verify if such intrusions are possible.

After simulating attacks, an assessment of the effectiveness of the defense measures is conducted to identify the most effective current security measures for the database system. This helps identify problematic areas and weaknesses that need improvement.

Using Results to Enhance Database Security. The final step in the attack modeling process is seeking ways to improve the protection of the database system. Based on the obtained results, decisions can be made regarding enhancing security policies, making changes to software, implementing security monitoring, and even increasing user awareness regarding data security.

Attack modeling on a database system occurs during the information security provisioning stage, assuming that threats can impact the system and how these impacts can be prevented or mitigated.

Data analysis of previous attacks is a process of studying and analyzing information about previous attacks or security incidents that occurred in a database system or similar organizations. This stage concludes with obtaining valuable experience and insights that can be used to enhance future protection. This method includes the following steps:

- Collecting data on previous attacks, incidents, or security events that occurred in the database system or other similar organizations. The process may involve information from event log records, incident reports, investigation results, etc.
- Analyzing typical attack scenarios, where typical attack scenarios identified in previous incidents are studied. this includes an analysis of the methods used by attackers to infiltrate the system, their objectives, and goals.
- Identifying common vulnerabilities involves the analysis of common vulnerabilities or weaknesses exploited by attackers in previous attacks, and identifying patterns indicating specific types of vulnerabilities that require attention.
- Studying and analyzing the scale of damage caused by previous attacks, including data loss, recovery costs, and other consequences. this analysis helps

improve risk assessment and make decisions regarding security measures.

- Evaluating the effectiveness of implemented measures, where the effectiveness of security measures implemented as a result of previous incidents is analyzed. studying this step helps improve and/or rectify security flaws in the database system.
- Developing a security improvement plan, which includes improvement procedures, implementation of new technologies and security measures, as well as staff training.

Continuous monitoring and updating of information about previous attacks should be carried out by the security service or database administrator. This process allows for timely responses to new threats and keeps the database system secure.

The analysis of data from previous attacks is a component of enhancing the security of database systems, after which problematic areas need to be identified and informed decisions regarding protective measures made.

Access rights analysis in a database system is the process of assessing and verifying the rights of users, user groups, and objects in databases. The assessment of access rights to the database, as well as control over them, is the culmination of the stage. It is crucial to verify who has access to the database, and what actions they can perform, and severely restrict these rights.

Identification of users and groups, which verifies identification data such as user logins and passwords, roles, and groups.

Authorization of users and groups, which verifies access rights to database objects, determines the actions users can perform in the database system, such as reading, writing, deleting, or modifying data, taking into account access levels and restrictions for different users and roles.

Access audit of database systems, which involves configuring the audit system to log access events to the database, including user logins and logouts, data changes, and other actions.

Monitoring and analysis of users include:

- Monitoring and analyzing audit events to detect suspicious or unusual activities.
- Continuous monitoring of user actions for abnormal or unusual activities.
- Analysis and response to negative actions, such as unauthorized access attempts or data modifications.

In light of the previous two processes (access auditing and user monitoring), the database system administrator needs to constantly review access rights, periodically checking and updating user and group access rights to changes in the organization, role structure, and security needs. It is important to remove or modify access rights for users who should no longer have access to the system.

Access rights analysis is a key component of ensuring the security of the database system, as it allows control and tracking of user access to data and protects the system from potential internal threats.

The method of determining protective measures and creating a response plan for external and internal threats. After identifying threats and assessing risks, a protection plan should be developed. Determining protective measures is a step in ensuring the security of the database system and answers the question, "How will we protect our data and infrastructure from external and internal threats?"

Determining protective measures is a stage in the risk modeling process where specific measures and strategies to reduce risk are defined to ensure the security of the database system. This stage requires careful analysis and planning and may include the following actions: selecting database protection measures, defining the responsibilities of security personnel, assessing the cost and resources of protection, and developing an implementation schedule for protective measures.

The selection of database protection measures involves defining specific security measures and technologies that can be implemented to protect the database system. This may include network protection, data encryption, authentication systems, and other measures.

Defining the responsibilities of security personnel involves assigning responsible individuals who will manage, implement, and monitor the security measures developed by the specified legislation for database security.

The assessment of the cost and resources of protection involves evaluating the costs associated with the implementation of selected security measures. This includes the cost of technologies, processes, personnel training, and other resources.

The development of an implementation schedule for protective measures is created to determine the timeframes for the implementation plan of necessary security measures and the sequence of their implementation, prioritizing security measures according to their importance and deadlines.

The incident response plan is a documented set of procedures and actions to ensure the security of operations in the event of a security incident. Creating an incident response plan involves developing a plan of action in the event of the detection of threats or security incidents, including recovery procedures and a return to normal operation. Such a plan includes the following elements:

- identification of incidents, defining what constitutes a security incident, and the events or actions that should trigger the activation of the response plan.
- response procedures for incidents, including a detailed description of the steps to be taken in the event of an incident, including contact persons to be notified and the sequence of actions to stop the incident and minimize damage.
- recovery plan detailing step-by-step actions for restoring normal operations after an incident. the improvement plan for security measures involves changing the security strategy, if necessary, based on updated risk data, in response to changes in threats and technologies.
- training and qualification enhancement for personnel regarding new security measures and security procedures for database systems.

Security testing is a fundamental process during which various types of attacks and intentional actions are carried out on a system to verify its resilience and the effectiveness of security measures, and to check its vulnerability and stability.

Examining security methods for database systems involves.

Penetration testing, where security experts attempt to enter the database using various attack methods, including SQL injections, session hijacking, authentication attacks, etc.

Vulnerability analysis involves identifying vulnerabilities and weaknesses in the database system that could be exploited by attackers.

Testing and assessing the effectiveness of protection involves conducting tests and checks of new security measures to determine their effectiveness and compliance with security requirements; addressing identified issues and improving security measures based on test results.

Testing also includes evaluating responses to incidents, assessing the system's protection, and how it reacts to different incidents. This evaluation includes checking the functionality of the event logging system and its monitoring.

Based on the results of security testing, plans for fixes and improvements are developed to eliminate identified vulnerabilities and enhance the security system. Continuous monitoring of security measures for abnormal activities and threat analysis, along with data analysis on security measures, allows for ongoing response to new threats.

Continuous Monitoring and Updates. Continuous monitoring and updates are extremely important aspects of ensuring the security of a database system. The database system needs to be constantly monitored to detect abnormal events and vulnerabilities. This may include monitoring event logs, analyzing network traffic, and other methods. The goal is to detect certain threats and respond to them before they can cause harm. Continuous monitoring and updates ensure that the database system remains resilient to new threats and provides a high level of data security. This allows organizations to operate in a reliable and secure environment, reducing the risks of data leaks and enhancing security.

4. Conclusions

Security modeling methods for database systems are a crucial component of contemporary practical information security. Analyzing data vulnerabilities helps identify weak points that malicious actors could exploit for unauthorized data access or database manipulation. Modeling attacks on the database system extends this analysis, aiding in predicting methods and strategies that attackers might employ.

Analyzing data from past attacks and incidents serves as a valuable source of information for studying patterns and threats targeting database systems. Approaches to access rights analysis assist in managing user privileges and developing access restriction strategies for database objects. Risk modeling and the identification of protective measures help assess existing threats and formulate plans to mitigate risks and enhance the security level of the database system.

Continuous monitoring and updates are essential since threats constantly evolve, and database systems must be prepared to detect and respond to incidents, as well as update security measures to adapt to new threats. These practices ensure reliable information protection and support data security in the modern information environment.

References

[1] I. Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2.

[2] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST) (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[3] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922

[4] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772181

[5] H. Shevchenko, et al., Information Security Risk Analysis SWOT, Cybersecurity Providing in Information and Telecommunication Systems 2923 (2021) 309-317.

[6] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.

[7] V. Astapenya, et al., Last Mile Technique for Wireless Delivery System using an Accelerating Lens, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (2020). doi: 10.1109/picst51311.2020.9467886.

[8] V. Astapenya, et al., Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems, in: 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772161.

[9] N. Shevchenko, et al., Threat Modeling: A Summary of Available Methods, Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2018).

[10] W. Xiong, et al., Cyber Security Threat Modeling Based on the MITRE Enterprise ATT&CK Matrix, Softw. Syst. Modeling 21(1) (2022) 157–177. doi: 10.1007/s10270-021-00898-7.

[11] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3188 (2022) 197–206.

[12] V. Pevnev, S. Kapchynskyi. Database Security: Threats and Preventive Measures, Modern Inf. Syst. 2(1) (2018) 69–72.