Micah Wieburg - Week 5 - Research Paper

Micah L Wieburg

School Of Computer Information Sciences, University of The Cumberlands

ITS834 - B04: Emerging Threats & Countermeasures

Dr. James Webb

November 17, 2022

Protecting sources of precious and necessary data is a high priority for all parties possessing such data. Databases are the foundation for data management, information organization, the ability to make decisions, and identifying valuable trends. Database systems are a resource that most of the population interacts with daily, making these systems vital to present-day life (Teimoor, 2021). With a heavy reliance on modern systems on databases, surrounding them with the proper security strategy is a task not to take lightly. Analysis of any database security strategy should show evidence of three constructs: confidentiality, integrity, and availability (Kriti, 2013). The three constructs of database security are threatened by numerous malicious attack strategies that must be counteracted and prevented with an educated database security strategy to mitigate the associated security risks. Risk analysis should be performed to identify all known and unknown threats to arrive at the proper security model. Another task in formulating a database security strategy is deciding upon a security model for the database system based on the risk analysis findings.

While risk analysis will help expose unknown security risks and threats, some basic database security strategies should be included in any strategy by default. Database auditing is an excellent component of database security that provides a valuable opportunity to track user activity. Database systems with auditing capabilities will follow successful and unsuccessful access attempts to a set of data (Teimoor, 2021). This process can bring attention to unusual and suspicious activity, potentially flagging a database access incident. Systems would also see significant benefits related to security by utilizing encryption (Teimoor, 2021). Although encryption has proven beneficial when applied to data while moving through a network, as this is where the information is most susceptible to intercept, it can also protect data while stationary (Teimoor, 2021). In the event data is accessed and extracted by an intruder, encryption will invalidate the data as it will be nearly impossible for the intruder to view the raw data (Sarmah, 2019).

Great database security strategy is also measured by how equipped the system is to evade common security threats. These threats include SQL Injection, Denial of Service, Excessive Privilege Abuse, and Backup Data Exposure (Teimoor, 2021). Each mentioned threat has good prevention strategies and should be incorporated into any database system seeking suitable security measures.

SQL Injection attacks occur when an attacker attempts to insert SQL into system queries via their input and should be thwarted by performing input validation and parametrized queries (Teimoor, 2021). Intrusion prevention technology should also be considered to aid in identifying the stored procedures and injection strings most susceptible to SQL injection (Sarmah, 2019).

Denial of service attacks is an attacker's attempt to halt system services, resulting in incoming requests being denied entrance to data and network resources. To prevent this impact, database systems should be configured to use intrusion prevention technology and operate only on necessary features (Sarmah, 2019). This approach will limit the number of services an attacker can target and keep the number of system resources requiring security to a minimum, lowering security risks.

Excessive Privilege abuse is associated with users taking advantage of their privileges over the database system to perform unethical actions. Adopting a query-level access control policy will aid in circumventing such a scenario. The granularity of the query level access control can go as far as limiting SQL operations at the table column level to prevent any malicious data manipulation by users with elevated privileges (Teimoor, 2021).

A Backup data exposure incident can occur if any storage device that contains database systems backups is impacted by theft. The best practice to prevent this exposure is encrypting backup data instances. In an effort to support this approach, many database management systems are crafted by vendors to disallow non-encrypted system backups (Teimoor, 2021).

Great database security measures are influenced mainly by how appropriate the implemented security models are for the database system and the data owner's preferences. Determining a suitable security model is guided by the examination of the different models available. Within the database security model, there is an excellent emphasis on access control to manage authorization. Authorization is the purpose of each security model (Penelova, 2021). The other attributes include subjects (human being, system process,.etc), objects (software resource), operations (action for requesting object access), permissions (what a subject can access), and policies (rules that approve/deny access requests (Penelova, 2021). There are several access security models available to establish organizational security. The following listings are presented to highlight the functionality of several standard models.

A security model that should be considered in every database system is access control lists. The main objective of access control lists is to restrict the capabilities and operations of authenticated users in a system (Kriti, 2013). Permissions are gathered and compiled into the respective access control lists (ACLs), which govern data access after being assigned to the user. The ACLs can determine the user's rights to retrieve or update data in the database to maintain the appropriate level of access to user roles (Teimoor, 2021).

The discretionary access control model is driven by object owners' ability to grant access permissions to their objects (Penelova, 2021). This approach provides pliability as the choice of authorized users is controlled by the database object owners and creators. Due to this flexibility, the DAC model is often not seen as a singular method of providing a secure system and is often paired with other security models.

The Role-based access control (RBAC) model is a widely used model built on the principles of assigning permissions to roles. Figure 1 illustrates the general layout of an RBAC-based system. Users, permissions, and roles are the essential elements of the RBAC model. Users are then assigned an appropriate role when the roles have been established and permissions are allotted. Within a corporation, the roles defined tend to be job responsibilities (Penelova, 2021). RBAC supplies uncomplicated maintenance since the permissions are at the role level and creates a single change point for making adjustments (Penelova, 2021). This amount of flexibility and focus on roles has allowed the RBAC model to become the most used access control model (Penelova, 2021).

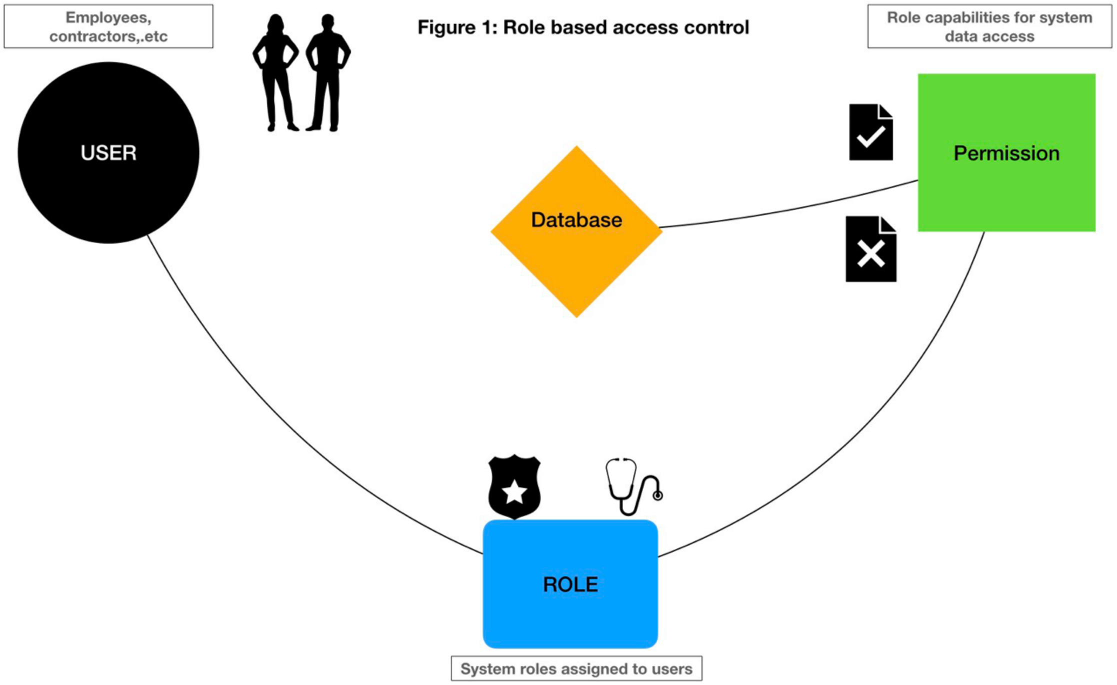

Figure 1: Role based access control

Employees, contractors,.etc
USER
Role capabilities for system data access
Permission
Database
ROLE
System roles assigned to users

Each object and subject of a system contains an associated set of attributes. The leverage this, an Attribute based access control (ABAC) model can be adopted to establish rules around objects. System subjects (humans, devices) attributes in a corporation typically consist of name, role, and job. The object is defined as the supplicated asset of the system, while a rule in ABAC is a policy that governs if a requestor can ingress an object. The mechanisms of the ABAC model analyze an object's attributes alongside the environment conditions (date/time, user location) and policies to finalize access decisions (Penelova, 2021).

Due to its importance and evolving threats, database security is an aspect of system design that requires constant evaluation. Applications rely on database systems' high availability, and confidence must be kept intact by ensuring data integrity. Ongoing strategies such as auditing and utilization of encryption support safeguarding the vital database systems for organizations and their users, both internal and external. Choosing the correct combination of access control models to regulate database security is a critical task in the overall approach to achieving good database security strategies and is a decision that must be made methodically.

References

Teimoor, R. A. (2021). A Review of Database Security Concepts, Risks, and Problems. *UHD Journal of Science and Technology*, *5*(2), Article 2. https://doi.org/10.21928/uhdjst.v5n2y2021.pp38-46

Kriti, I. K. (2013). Database Security & Access Control Models: A Brief Overview. *International Journal of Engineering Research*, *2*(5), 9.

Sarmah, s. (2019). Database Security –Threats & Prevention. *International Journal of Computer Trends and Technology*, *67*, 46–53. https://doi.org/10.14445/22312803/IJCTT-V67I5P108

Penelova, M. (2021). Access Control Models. *Cybernetics and Information Technologies*, *21*(4), 77–104. https://doi.org/10.2478/cait-2021-0044

Mousa, A., Karabatak, M., & Mustafa, T. (2020). Database Security Threats and Challenges. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS49300.2020.9116436