Database Access Controll
Jonathan Steelman
Columbus State University
CPSC6126

Abstract- Database access control is a vital part to not only database security but to the overall system security. An unauthorized user should not be allowed full access to a database the entire program can be compromised if the user has proper knowledge, but this is something we can’t risk. That is why it is crucial that the database have limitations for different users that limits what that user can or can’t do. In this paper we will discuss different access control models, and each models advantages and disadvantages.

Keywords—database; access; control; user based; view based; schema’s

I. INTRODUCTION

There are many ways that you can protect your database from outside intrusion. The most trusted and most frequently used ways to protect your database from outside intrusion is with database access control. Database access control varies greatly depending upon the database requirements. For example database access control can be as simple as only allowing certain users to connect to a server to as complicated to allowing different users to have different privileges in which they can access and modify the database.

Database access control and database protection is a vital aspect of the overall system security. This is a very important subject because it can effect each and every one of us. How many times in the last year have you heard of a company getting compromised and their customer’s credit card and or personal information is lost. Some of these incidents was where an unauthorized user gained access to a “secure” database. There need to be limitation/rules for what users can access and which users are authenticated for proper system protection. We don’t want unauthorized users because if an educated unauthorized user gains access to our database they can gain access to the information or corrupt the database. We also need to protect what the authenticated users can access because we need to ensure that our sensitive data does not get accessed/modified by an authenticated user who should not be able to access the information.

There are two main versions of database access control implementation which are view based access control and user based access control. View based access control is not based off of roles or the characteristics of users [4]. Instead of using roles they consider specific conditions that are either class, object, or resource based [4]. For example you have three separate views that access a database. Each view returns slightly different data depending upon what data the client is allowed to see. So one user/view might be only able to see basic information while other is allowed unrestricted access to the database. Each view has a subsequent select statement under the hood so by calling the view it only returns a certain subset of data [1]. This is a very basic understanding and does not allow updates to the database only select statements.

User based access control limits the users by a set of roles and schema’s. There are two distinct parts to user based access control, roles which are where certain users have more control/manipulation to the DB, and schema’s which all users of that type are allowed to access all the objects/data for that schema [3]. There are two distinct users of the database, a super user who has advanced powers typically called a database administrator or DBA for short [2]. The second type of users are the users that typically access the data. Saw we are building a database containing airplane and parts. We have one users (fighter) that has access to the military airplane parts catalog. We have a second user (aircraft) that has access to non-military airplane parts. The different users will help differentiate the sensitive military parts with the regular aircraft parts.

The second way you can control access to a database with users is by schemas. Schemas are a global array that can contain main database objects [3]. A schema can contain users, database tables, views and much more. Think of a schema as a Toyota car, the car contains multiple different objects and parts but they are all contained in the Toyota car. In order to access the car (schema) you need the Toyota key. If you have the key you can access anything in that car (schema). The same general rules apply for the
database, only certain users can access the schema and can only access the information schema allows [2]. There can be multiple schemas that contain the same tables. Sticking with the airplane example discussed earlier we have two schema’s aircraft and fighter. In both of these schema’s we have tables like fuselage and tires because they are general parts to all aircraft. In the fighter schema we have tables such as weapons which are specific only to the military schema. You can see how the schema allows different users to update the same tables but still allowing special conditions for specific schema requirements.

II. RELATED WORK

There has been a vast amount of research done on the different database access control methods. There has been entire books and many products such as Oracle and MySQL has published paper/journals on the best security implementation practices. These best practices usually go into great detail exactly what each and every component does and how you can configure it [5]. So you can see for example what the schema is, what it contain, and how you can configure the schema to work in your project [5]. This is very pertinent information which a can be used to greatly improve the security of your database and installation.

III. PROBLEM STATEMENT

There are so many items that are needed to fully protect your database from outside intrusion. These requirements range from physical database security concerns to employee back ground checks. We can only the database access control methods in that schema. Each different database access control methods has its own advantages and disadvantages. Each was designed for its own specific needs and can be tailored for nearly any database requirements. The main problem is what database access control method you pick for your task. There are so many options and choices and they can be applied to almost any database. Regardless if you’re using MySQL on Windows or Oracle in Linux these databases access control methods can be applied. There are only two accepted database access control methods, view based data access control and user based database access security modules. Each different access control model has its own set of advantages and disadvantages. We will also discuss which database access control module is better suited for a certain system size and system requirements.

IV. PROPOSED SOLUTION

The main issue that we have when choosing which database access method is which method is best for our system. They all have their advantages and disadvantages and some work better in particular environments but first we will discuss their advantages. View based database access control has the distinct advantage of being the simplest to set up. You don’t worry about different users or database schema’s, you just need to know which data each view can access and then you will build views with specific select statements under the covers that only allows a certain subset of data to be returned for that particular view [1]. This is very easy to set up and is great for smaller less complicated systems because they don’t need all the added features that come with user based database access control methods [4]. User based database access control has the distinct advantage of being more customizable to better meet the needs of the database [3]. Not only does the user access control already contain roles and schema access control but there can be views inside the schema [3]. So not only do you have all the different access control roles based off of users and schema but you still have all the view functionality included. It has all the all functionality of view with all the customization of user based access control, it is the ideal interpretation for big complex database.

Each database access control method also has disadvantages associated with them as well. View based access control might be very easy to set up and use but ultimately isn’t the end all solution. It might be a great way to control the database on smaller systems but unfortunately isn’t up to the task in larger more complex systems. There are too many special requirements that view based access control is better suited as a component of database security and not the only database access control policy [4]. User bases access control is very customizable and able to handle any special security needs but is often complex to set up. All that customizable and special features come at a cost and you really need to know what exactly you need or you can find yourself lost in the complex set up [3].

V. CONCLUSION AND DIRECTIONS FOR FURTHER WORK

This paper gives a review about both view based data access control and user based database access security modules. With user based database access
control you have roles and schemas to monitor and ensure your database is protected. Unfortunately each database access control method recommended in this paper has its own limitations. Each database access control has its own advantages and disadvantages associated with it. These advantages and disadvantages can aide in choosing what method is the best accessing method but ultimately is completely dependent upon the system. Simple systems may be able to get away with just view access control but more complicated systems may need the user based access control. Instead of using roles view based database access control they consider specific conditions that are either class, object, or resource based [4].

It is entirely dependent on the data and what exactly is needed from the system requirements perspective. I think it would be a great benefit to the entire community to analyze the different database access methods are there practical applications in terms of system size and security requirements. There should be a complete analysis of any and all database access control methods and where each database access control method is the most efficient method.

REFERENCES


