# Option #1 : Securing the Database Environment

Liam Bergerson

CSU - Global

ITS411-1

D. Morrill

4/10/22

## Option #1 : Securing the Database Environment

Haphazard Inc. is a company that has recently hired me as a Database Administrator (DBA). They have asked me to create multiple users, roles, and privileges that will be added to the database. Additionally, they have asked me to recommend methods of authentication and authorization they can use to increase the security of their database. Policies will be developed to ensure employees are being secure during their operations.

### Authentication and Authorization

The goal of authentication is to make sure that the user that is trying to access the database is who they say they are and not an unauthorized user (Castro, 2018). There are multiple methods that can be used to authenticate a user into a database. The first method is a simple username and a password. This method is the basis of authentication; a user puts in their username to signify who they are, and then they put in a password that verifies that it's the authorized user. However, this method is only as good as the password. That means that if a weak password is used, the account is easy to breach. If the password is strong, it's much more difficult to breach the account.

The second method is Multi-factor Authentication (MFA). MFA is an extra layer of security that will prompt the user to complete another step in order to fully access the account. When logging into an account, after putting in the username and password, you have to put in a code that has been sent to the user via text message or a third-party authentication application (Alliance, 2021).

The third method is token-based authentication. With token-based authentication, the user inputs a password, then a token will be generated. That token is encrypted and

has a life span. During the lifespan, the user does not have to re-enter their credentials in order to access the website again. Once the token has expired, the user will have to re-enter their credentials in order to generate a new token.

MFA is the method that will be used along with a username and a password for Haphazard Inc. MFA is easy to use and excellent for security. Even if the user uses a weak password for their account, a hacker will not be able to get into the account without the code generated by text message or a third-party application. It's almost like a safety net; the account will still be protected while the user creates a much stronger password for their account.

In terms of authorization, the principle that Haphazard Inc. will adapt is the principle of least privilege. Users of a database can only view the data they are authorized to view, any other data cannot be seen or interacted with unless you have the proper authorization (Castro, 2018). The principle of least privilege will ensure that users have only the privileges and authorization they need to do their job and nothing more. This will increase security for the company because there are far fewer accounts that have full access that hackers look for when they want to steal data.

## Policies

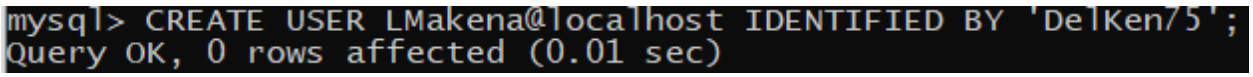
Two policies will be used to maintain security of this company: a password policy and an acceptable use policy. A password policy will explain to users how a password should be used and will require users to follow this policy. A good password policy must define what a strong password is, when a password should be changed, and require users to not reuse a password they have already used. A strong password must be eight or more characters and include upper and lowercase letters, numbers, and special

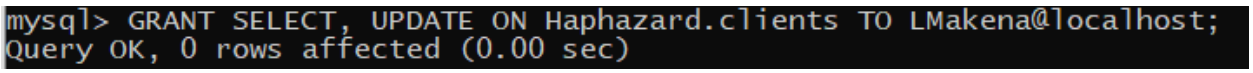
characters. A password must be changed every few months. Finally, a password must never be reused when changing passwords.

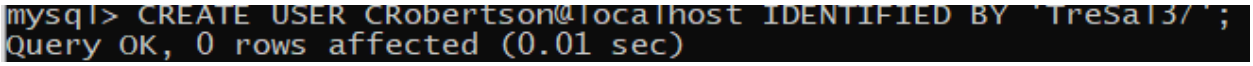
An Acceptable Use Policy (AUP) defines standards of behavior for users when they use company hardware and software (Kostadinov, 2014). It basically tells users to only use company equipment for work and any software or data is only used for work purposes. This policy increases security because if employees are using their computer for work and work only, the risk for breach is lower because interaction is within the network and not outside. However, if the internet is used for leisure browsing the chance for a user to click on a malicious website is much greater than if they are browsing the website for work purposes.

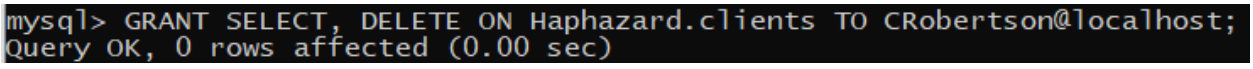
**Creating Users**

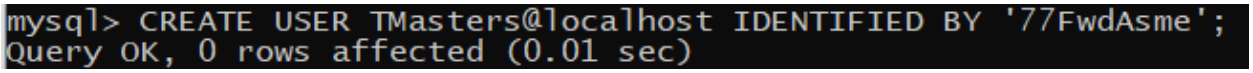
Users, roles, and privileges will be added in a MySQL database. Here are screenshots of the users, roles, and privileges being added.

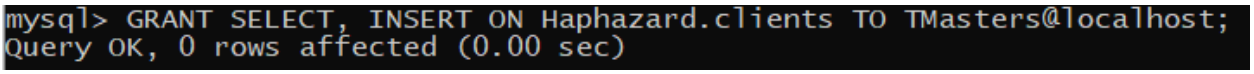


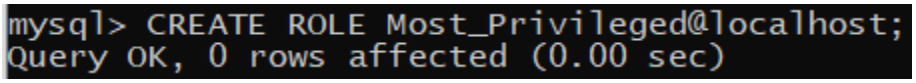



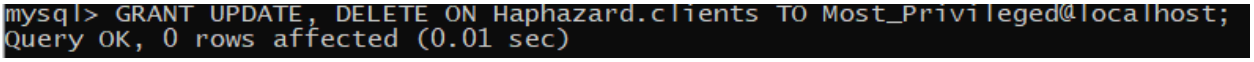



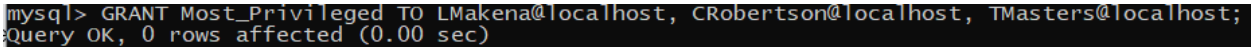






## Conclusion

Haphazard Inc. has been given multiple methods of which to increase security for their company. Multi-factor Authentication (MFA) will be used as an extra layer of security along with usernames and passwords. If a weak password is used, the hacker cannot get into the account without the code generated by text message or a third-party application. The principle of least privilege will ensure that users are given authorization for only data that they require to work, nothing more. A password policy and an Acceptable Use Policy will ensure that users use passwords properly and only to use company equipment for work. Finally, users, roles, and privileges have been created in MySQL for haphazard's databases.

## References


Alliance. (2021, February 21). *5 Common Authentication Methods For Network Security*. Alliance Technology Partners. https://www.alliancetechpartners.com/network-security-authentication/

Castro, K. (2018, August 3). *Security, Integrity and Authorization in DBMS*. Tutorialspoint. https://www.tutorialspoint.com/Security-Integrity-and-Authorization-in-DBMS

Kostadinov, D. (2014, Sep 23). *The essentials of an acceptable use policy*. Infosec Resources. https://resources.infosecinstitute.com/topic/essentials-acceptable-use-policy/