Eric Zorn

10.1.2017

ICT 4300

Professor/Dr. Lakhani

Module 4: Authentication and Authorization Discussion Questions

1. What is Authentication?
   1. Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. Tech Target says that the AAA server compares a user’s authentication credentials with other user credentials that had already been stored into the database previously. Currently, we are using biometrics as our focus on user authentication in addition to two step verification and username/password needs. Many technology companies are ensuring that their products can now read and store user’s fingerprint’s or even their facial structure in order to grant access to a system. Many companies however, do not store biometric data onto a server and only locally onto the device. This is done for security and privacy of the user as well as the prevention of hackers stealing this highly sensible identity information from a server. This could be catastrophic if biometrics were ever stored and stolen from a server.
2. What is Authorization?
   1. The following definition is also given by Tech Target. Authorization is something that has to be gained by the user in order to accomplish certain tasks in the web page or application. After logging into the system, the user may try and state some commands. The program on the back-end determines the authorization status of the user and if that user has the right to make those certain commands. Examples of this might be the admin to a system versus a standard/general user of the system. Authorization is the process of enforcing policies by determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. In other words, this will happen simultaneously with the authentication of the user credentials. Every user has a different level of authorization and will be granted access to only specific parts of the system. In rare cases, if they are the admin to the system, they might have complete control over any system component that they wish to manipulate.
3. How is authentication different from authorization?
   1. Both authentication and authorization are very similar and stem off one another, however, they are different in their own ways. Once the user has created an account and store their information to the sever, the next step is the authentication. Authentication is the algorithm that will check the input values upon the submit action from the user. The user authentication algorithm will link to the database and try and see if the user credentials are identical to the ones entered from the user. In most cases, this is commonly just a username and a password. For extra authentication practices, some companies will ensure that the user had re-entered the same exact password. Companies like Apple are partaking in the newer trend of two-step verification. The first step is to match the database information from the server to the user input field values. The second step is for a randomly generated code to be sent to the user’s phone number. If both the form values and the randomly generated code will match, the user is then “authorized” to use the application. This is where the term authorization comes into play. After the user has been authenticated and authorized login to the system, the system will then check their account type. Like I had mentioned in the previous question, if the user is a general user, they will only be allowed to use the most general components of the system. To use the Canvas example, the user as a student is allowed to simply view their course, upload any homework assignments, and or converse in discussion posts with other students or professors. The next tier of the authorization type would be a professor. The professors are allowed to post the class criteria and grade assignments, keep items in the calendar, change the syllabus or welcome page and many other features. All of this has been authorized solely for the professor while the student does not have the authorization to manipulate any of this information or these components in the system. Lastly, there is the system administrator. He or she has complete control over the system and its components. They can see any changes made by the professor or the student, as well as, they can make any changes to the system that they would like as well. They also have the right to update and add or remove any possible software components. Many web applications are built using component based frameworks now in JavaScript for authorization and easier implementation needs like Angular or React.
4. What is Accounting?
   1. Accounting is third plank in the AAA framework (Authentication, Authorization, and Accounting). It measures the resources a user consumes during access. Tech Target mentions that this can include the amount of system time or the amount of data that a user has sent and/or received during a session. Accounting is carried out by logging of the session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities. Many of these accounting services can be provided from a dedicated AAA server that will provide this computer system with the needed accounting functionalities. Also according to Tech Target, one of the current standard by which network access servers interface with the AAA server is the Remote Authentication Dial-In User Service (RADIUS).
5. What is the importance of accounting?
   1. For this definition of accounting, or any other financial definition of accounting, this can be extremely important for record keeping. In an application or programming environment, people want to have the insurance that their billing cycles, database information, time spent, information searched or just about anything else is stored and ensured to work properly. Examples of accounting in the digital industries that might be considered to be debatable is the information storage from browsing and interactivity information. Google has been under much scrutiny from the world because of their privacy infringement. They have been known to monitor and account for all data uploaded to their Google Drive cloud servers as well as any message and attachment information in Gmail. This allows Google to target any information or advertisements to the user. Accounting information is what will ensure proper authentication and authorization from the database as well. It also allows for the company or the developer to be able to track their information for data analytics as well, which is one of the most powerful industries now a days.