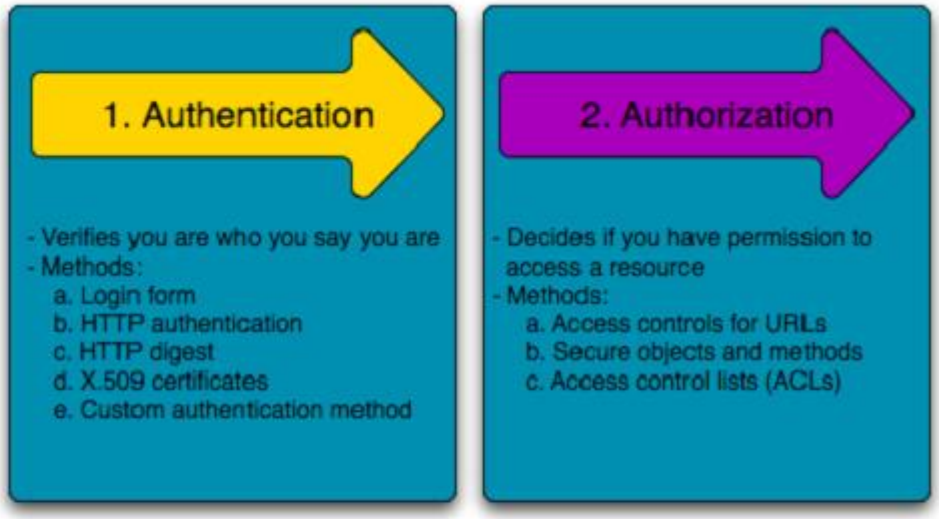
Difference between Authentication and Authorization



- Verifies you are who you say you are
- Methods:
  - a. Login form
  - b. HTTP authentication
  - c. HTTP digest
  - d. X.509 certificates
  - e. Custom authentication method

- Decides if you have permission to access a resource
- Methods:
  - a. Access controls for URLs
  - b. Secure objects and methods
  - c. Access control lists (ACLs)

Both the terms are often used in conjunction with each other in terms of security, especially when it comes to gaining access to the system. Both are very crucial topics often associated with the web as key pieces of its service infrastructure. However, both the terms are very different with totally different concepts. While it’s true that they are often used in the same context with the same tool, they are completely distinct from each other.

Authentication means confirming your own identity, while authorization means granting access to the system. In simple terms, authentication is the process of verifying who you are, while authorization is the process of verifying what you have access to.

Authentication

Authentication is about validating your credentials like User Name/User ID and password to verify your identity. The system determines whether you are what you say you are using your credentials. In public and private networks, the system authenticates the user identity via login passwords. Authentication is usually done by a username and password, and sometimes in conjunction with factors of authentication, which refers to the various ways to be authenticated.

Authentication factors determine the various elements the system use to verify one's identity prior to granting him access to anything from accessing a file to requesting a bank transaction. A user's identity can be determined by what he knows, what he has, or what he is. When it comes to security, at least two or all the three authentication factors must be verified in order to grant someone access to the system.

Based on the security level, authentication factor can vary from one of the following:

- **Single-Factor Authentication** – It's the simplest authentication method which commonly relies on a simple password to grant user access to a particular system such as a website or a network. The person can request access to the system using only one of the credentials to verify his identity. The most common example of a single-factor authentication would be login credentials which only require a password against a username.
- **Two-Factor Authentication** – As the name suggests, it's a two-step verification process which not only requires a username and password, but also something only the user knows, to ensure an additional level of security, such as an ATM pin, which only the user knows. Using a username and password along with an additional piece of confidential information makes it virtually impossible for fraudsters to steal valuable data.
- **Multi-Factor Authentication** – It's the most advanced method of authentication which uses two or more levels of security from independent categories of authentication to grant user access to the system. All the factors should be independent of each other to eliminate any vulnerability in the system. Financial organizations, banks, and law enforcement agencies use multiple-factor authentication to safeguard their data and applications from potential threats.

For example, when you enter your ATM card into the ATM machine, the machine asks you to enter your pin. After you enter the pin correctly, the bank then confirms your identity that the card really belongs to you and you're the rightful owner of the card. By validating your ATM card pin, the bank actually verifies your identity, which is called authentication. It merely identifies who you are, nothing else.

Authorization

Authorization, on the other hand, occurs after your identity is successfully authenticated by the system, which ultimately gives you full permission to access the resources such as information, files, databases, funds, locations, almost anything. In simple terms, authorization determines your ability to access the system and up to what extent. Once your identity is verified by the system after successful authentication, you are then authorized to access the resources of the system.

Authorization is the process to determine whether the authenticated user has access to the particular resources. It verifies your rights to grant you access to resources such as information, databases, files, etc. Authorization usually comes after authentication which confirms your privileges to perform. In simple terms, it's like giving someone official permission to do something or anything.

For example, the process of verifying and confirming employees ID and passwords in an organization is called authentication, but determining which employee has access to which floor is called authorization. Let's say you are traveling and you're about to board a flight. When you show your ticket and some identification before checking in, you receive a boarding pass which confirms that the airport authority has authenticated your identity. But that's not it. A flight attendant must authorize you to board the flight you're supposed to be flying on, allowing you access to the inside of the plane and its resources.

Access to a system is protected by both authentication and authorization. Any attempt to access the system might be authenticated by entering valid credentials, but it can only be accepted after successful authorization. If the attempt is authenticated but not authorized, the system will deny access to the system.

Authentication	**Authorization**
Authentication confirms your identity to grant access to the system.	Authorization determines whether you are authorized to access the resources.
It is the process of validating user credentials to gain user access.	It is the process of verifying whether access is allowed or not.
It determines whether user is what he claims to be.	It determines what user can and cannot access.
Authentication usually requires a username and a password.	Authentication factors required for authorization may vary, depending on the security level.
Authentication is the first step of authorization so always comes first.	Authorization is done after successful authentication.
For example, students of a particular university are required to authenticate themselves before accessing the student link of the university's official website. This is called authentication.	For example, authorization determines exactly what information the students are authorized to access on the university website after successful authentication.

Summary

Although, both the terms are often used in conjunction with each other, they have totally different concepts and meanings. While both of the concepts are crucial to web service infrastructure, especially when it comes granting access to a system, understanding each term in regards to security is the key. While most of us confuse one term with another, understanding the key difference between them is important which is actually very simple. If authentication is who you are, authorization is what you can access and modify. In simple terms, authentication is determining whether someone is who he claims to be. Authorization, on the other hand, is determining his rights to access resources.